Riku Santeri Aittokallio

EU:n tietosuojan kokonaisuudistus

Opinnäytetyö
Kevät 2017
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Riku Aittokallio

Työn nimi: EU:n tietosuojan kokonaisuudistus

Ohjaaja: Alpo Anttonen

Vuosi: 2017 Sivumäärä: 42

Tämän opinnäytetyön aiheena on Euroopan unionin uusi tietosuoja-asetus, joka astuu virallisesti voimaan vuoden 2018 ensimmäisellä puoliskolla. Tavoitteena on selvittää miksi kyseinen muutos tehtiin, millaisia muutoksia siitä aiheutuu, kuinka ne poikkeavat vanhemmista asetuksista ja kuinka muutokset vaikuttavat yrityksiin, rekisterinpitäjiin sekä yksityishenkilöihin. Lisäksi kädään läpi ongelmia, joita lainsäädännön muutos toi mukanaan.

Muutoksia pyritään tutkimaan mahdollisimman monelta kannalta, mutta erityisesti työssä keskitytään rekisterinpitäjän ja rekisteröidyn kohdalla tapahtuviin muutoksiin. Rekisteröidyn osalta tutkitaan uusia oikeuksia sekä mahdollisuuksia vaikuttaa omien henkilötietojen keräämiseen ja käsittelemiseen. Rekisterinpitäjän kannalta tutkittaan uuden asetuksen asettamia tavoitteita, velvoitteita, sanktioita ja käydään läpi muutoksia nykyiseen tietojen käsittelyyn verrattuna. Työssä tarkastellaan asiaa myös suuremmasta näkökulmasta, ensin Suomen ja sitten Euroopan kannalta. Lopussa tehdään vielä yhteenveto ja pohditaan asiaa ja sen herättämiä ajatuksia.

Avainsanat: Tietosuoja, rekisterinpitäjä, rekisteröity, tietosuoja-asetus

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Data Communications Technology

Author: Riku Aittokallio

Title of thesis: Renewal of EU data protection regulations

Supervisor: Alpo Anttonen

Year: 2017 Number of pages: 42

The topic of this thesis was the new general data protection regulation of European Union, which will come into effect during the first half of the year 2018. The objective was to answer such questions as why the new regulation was created, what kind of changes it will bring, how the new regulations will differ from the current ones and how the changes will effect companies, data controllers and individuals across Europe.

The aim was to view the effects of the new regulations from as many perspectives as possible but the thesis concentrated more on the changes that will effect data controllers and registered users. From the perspective of a registered user, the thesis studied the new rights of individual users and their possibilities to have an effect on the collecting and use of their personal information. From the perspective of a data controller, the thesis concentrated on the goals, responsibilities and sanctions and studied the changes compared to the current regulations. This thesis also viewed the changes in a bigger scale, first from Finland's and afterwards from Europe's perspective. In the end, there was some speculation on the topic and a conclusion.

Keywords: Data security, data controller, registered customer, data protection regulation

SISÄLTÖ

Kuvaluettelo

Käytetyt termit ja lyhenteet

Biometrinen	Biometrinen tarkoittaa biologista, esim. biometrisessä passissa on siru, johon on tallennettu passin omistajan biologisia tietoja, kuten kasvokuva tai sormenjälki.
Digitalisoituminen	Siirtymistä teknologiapainotteiseen elämäntyyliin. Tieto kulkee internetin kautta, uutiset löytyvät netistä, passeissa on siru, johon on tallenettu henkilön tietoja.
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto).
Profilointi	Tapa jakaa ihmisiä pieniin ryhmiin esmierkiksi ihon värin, koulutuksen tai seksuaalisuuden perusteella.
Rekisterinpitäjä	Luonnollinen tai oikeushenkilö, julkinen viranomainen, viraasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
Rekisteröity	Henkilö, jonka henkilötietoja käsitellään.
Tietosuoja	Tietosuojalla tarkoitetaan ihmisen henkilötietoihin ja toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista, jotta henkilön yksityisyys voitaisiin taata.
Tietosuojaseloste	Internetissä ennen henkilökohtaisten tietojen, kuten paikannustietojen keräämistä tapahtuva toimenpide, jossa käyttäjää pyydetään hyväksymään tietojen kerääminen. Kertoo tietojen luovuttajalle tämän oikeudet.
Tietosuojavastaava	Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä, mikäli tietojen käsittelyä suorittaa viranomainen tai muu julkishallinnon elin, joka ei ole tuomioistuin. Ydintehtävät

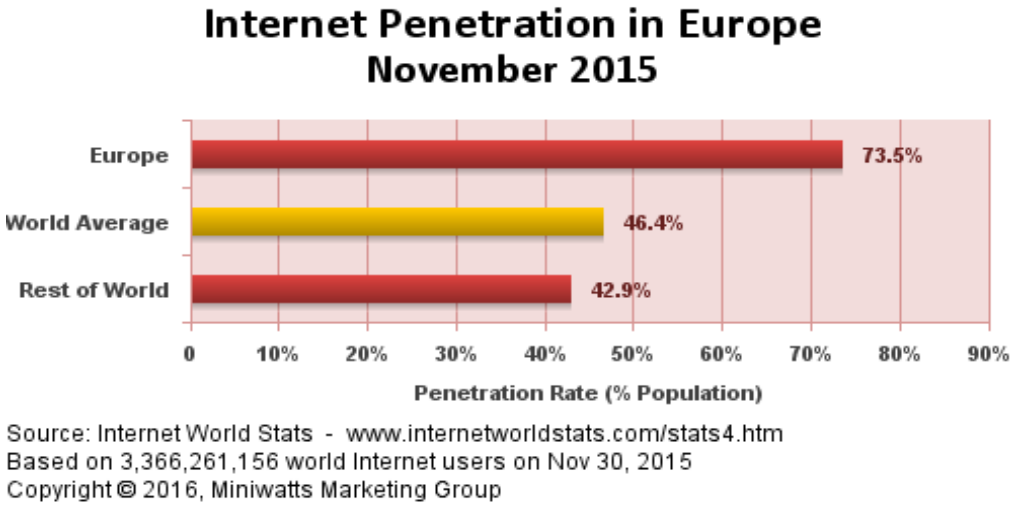
	vaativat rekisteröityjen säännöllistä seurantaa tai ydintehtävät kohdistuvat erityisiin tietoryhmiin esim. rikostuomioihin.
Tietoturva	Kaikki mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilyttämiseen käsittelyn aikana.

1 JOHDANTO

1.1 Mitä on tietosuoja

Internet on kasvavassa osassa jokapäiväistä elämää. Sosiaalisen median valtakausi on alkanut ja ihmisillä on tarve pysyä kytköksissä toisiinsa internetin luoman verkon kautta. Myös henkilötietojen käsitteleminen on arkipäiväistynyt; verkkokaupoista tilaaminen ja sosiaalisessa mediassa tiedon jakaminen on päivä päivältä yleisempää. Henkilötietoja luovutetaan enemmän kuin olisi tarpeen ja tietosuojaselosteet ohitetaan rastittamalla ”Hyväksyn palvelun ehdot”-ruutu sen enempää asiaa miettimättä. Samanaikaisesti mediassa kohutaan tietovuodoista, joissa pahinmillaan miljoonien käyttäjien henkilötiedot ovat vuotaneet julkisuuteen. Mitä tahansa internetissä tehdään, jää siitä aina digitaalinen ”jalanjälki”. Osaava ihminen voi näitä jälkiä seuraamalla saada tietoja, joita ei julkisuuteen haluta.

Eurooppalaiset ovat pohjoisamerikkalaisten lisäksi maailman ahkerimpia internetin käyttäjiä. Internet World Stats julkaisi vuoden 2015 lopussa raportin, jonka mukaan lähes koko Pohjois-Euroopan väestö käyttää internetiä. Esimerkiksi Suomen väestöstä 93,5 %, Ruotsista 94,6 % ja Norjasta 93,6 % väestöstä käyttää internetiä.



Kuva 1. Internet Penetration in Europe November 2015.
(Internet World Stats 2015)

Kaikilla on oikeus tietosuojaan. Jokainen on täysin oikeutettu tietämään ja päättämään, miten kerättyjä henkilötietoja käsitellään. Jokaisella on myös oikeus elää omaa elämäänsä ilman, että siihen puututtaisiin perusteettomasti. Tämän lisäksi jokaisen oikeuksiin kuuluu se, että tilanteen vaatiessa tätä kohdellaan oikeellisten tietojen pohjalta ja muiden perusoikeuksien mukaisesti. (Aarnio 2015.)

1.2 Opinnäytetyön tavoite ja tarkoitus

Opinnäytetyön tarkoituksena on tutkia, selvittää ja pohtia EU:n uuden tietosuoja-asetuksen mukanaan tuomia muutoksia ja niiden vaikutuksia yrityksen ja yksityishenkilön kannalta. Työ pohjautuu tekijän omaan mielenkiintoon eikä sillä ole toimeksiantajaa.

Tavoitteena on kerätä yhteen aiheeseen keskeisesti liittyviä käsitteitä, periaatteita ja lainsäädäntöä, sekä tutkia ja pohtia niitä ja niistä aiheutuvia muutoksia yksityishenkilöiden ja yritysten kannalta.

Aiheeseen perehdytään Euroopan parlamentin ja neuvoston uuden tietosuoja-asetuksen (EU 2016/679), Henkilötietolain (Henkilötietolaki 523/1999), sekä Euroopan parlamentin ja neuvoston direktiivin (EU 95/46/EY) kautta.

1.3 Työn rakenne

Ensimmäisessä luvussa kerrotaan lukijalle mistä opinnäytetyössä puhutaan ja mitkä ovat sen tavoitteet. Toisessa luvussa selvitetään mihin uudella tietosuoja-asetuksella pyritään. Tämän jälkeen käydään läpi muutoksen kannalta tärkeitä lainsäädännöllisiä kohtia ja selvitetään vielä tarkemmin miten muutokset tulevat vaikuttamaan organisaatioihin ja yksityishenkilöihin. Neljäs luku selvittää muutosten vaikutuksia isommassa mittakaavassa, ensin Suomen ja sitten Euroopan kannalta. Työn lopusta löytyy yhteenveto ja pohdinta.

2 HENKILÖTIEDOT KÄSITTELYSSÄ: TARKOITUS JA MÄÄRITELMÄT

Valtioiden välinen yhteistyö lisääntyy jatkuvasti. Tämän vuoksi myös tietoa liikutetaan enemmän ja nopeammin. Vuonna 2015 Schengen-maiden välille luotiin yhteinen viisumitietojärjestelmä, jonka avulla viranomaiset pääsevät käsiksi kaikkiin Schengen-alueelle viisumia hakevien henkilöiden tietoihin. (Ulkoasiainministeriö 2015.) Henkilötietoja kuljetetaan myös monissa eri muodoissa. Edellä mainitussa esimerkissä viranomaiset saavat käyttöönsä henkilöiden biometrisiä eli biologisia henkilötietoja, kuten kasvokuvan tai sormenjäljen.

Henkilötietojen kerääminen hyödyttää yrityksiä. Esimerkiksi internetissä toimivat kaupat, kuten Ebay ja Amazon keräävät käyttäjien selaushistoriaa ja hakusanoja, jonka seurauksena sivustot mainostavat kävijöille tuotteita aiemmin haettujen tulosten perusteella tavoitellakseen lisää myyntiä. Henkilötiedot saattavatkin olla arvokkainta aineetonta omaisuutta yrityksille. (Lehtonen 2014.)

2.1 Uuden tietosuoja-asetuksen periaatteet

Tietosuojalla pyritään velvoittamaan rekisterinpitäjää huomioimaan henkilötietolaki (Henkilötietolaki 523/1999) sekä erityislait toiminnassaan. Tietosuoja tarkoittaa myös yksityisyyden suojan turvaamista. Asetuksen tarkoituksena ei suoranaisesti ole henkilötietojen suojaaminen, vaan rekisterinpitäjän ohjaaminen tietojen vastuulliseen käsittelemiseen. Perustuslaki määrittelee Suomen kansalaisille yksityiselämän suojan. Uusi tietosuoja-asetus pyrkii suojaamaan rekisteröidyn käyttäjän yksityiselämää ja oikeuksia. (Andreasson, Koivisto & Ylipartanen 2016, 18.)

Henkilötietolaki toimii rajojen määrittäjänä rekisteröidyn henkilötietojen käsittelyssä. Tietosuojaa voidaan miettiä tiedollisena kotirauhana sekä työkaluna luottamuksen rakentamiseen. Esimerkiksi verkkokaupoissa ostajat ja myyjät rakentavat luottamusta tietosuojan kautta. (Andreasson ym. 2016, 18.)

Tietoturvasta puhuttaessa tarkoitetaan toimenpiteitä, joiden kautta pyritään parantamaan yritysten tai henkilöiden yksityisyyden turvaa ja oikeuksia. Nämä eivät ole kuitenkaan ainoita toimenpiteitä, vaan myös tiedon laadun, luottamuksellisuuden ja eheyden säilyttäminen ovat keskeisessä osassa tietoturvaa. Tietoturvan tarkoituksena on pyrkiä estämään luvattomien henkilöiden pääsy tietoihin, tietojen poistaminen tai muokkaaminen ja vahinkojen minimointi. Tästä syystä tietosuojaa pyritään toteuttamaan tietoturvan kautta. (Andreasson ym. 2016, 18.)

Suomen perustuslaki määrittelee itsemääräämisoikeuden, joka antaa henkilölle oikeuden määrätä itseensä liittyvissä asioissa. Yksityiselämän suoja antoi idean itsemääräämisoikeuden liittämisestä henkilötietojen suojaan. Päämäränä on antaa henkilölle mahdollisuus päättää itse, miten hänen henkilötietojaan käsitellään. Mutta onko tietosuoja tarpeellista? Toisen maailmansodan aikana ihmisten tietoja rekisteröitiin reikäkorteille Saksassa. Näiden korttien perusteella etsittiin muun muassa juutalaisia kekitysleireille. Tietojen rekisteröimistä ja käsittelyä on myös pidetty ihmisarvoa alentavana. (Neuvonen 2014, 59.)

Tietojen rekisteröiminen ja käsittely on kuitenkin välttämätön paha hyvinvointipalveluiden takaamiseksi. Ilman tietojen keräämistä ei olisi passeja, terveydenhuollon rekistereitä tai sähköisiä maksuvälineitä. On siis välttämätöntä, että osasta yksityisyyttä luovutaan, mutta tämän takia luotiin uutta asetusta henkilötietojen suojaamiseksi. Tarvitaan rajat joiden puitteissa tietoja voidaan käsitellä. Henkilötietojen suoja voidaan jakaa kahteen eri ulottuvuuteen. Vertikaalisuhteessa suojataan ihmistä valtion liialta yksityisyyteen puuttumiselta, kun taas horisontaalinen ulottuvuus näkyy tietojen suojassa siten, että rekisterinpitäjällä on velvollisuuksia käsitellä tietoja. (Neuvonen 2014, 60.)

Myös yrityksen on opittava muuttamaan ajattelumalliaan. Tieto on nykyisin tuotannontekijä ja sen ympärille rakentuu jatkuvasti uusia palveluja. Yritysten ja henkilöiden on siis otettava yhä enemmän huomioon verkkoympäristön tietoturvapuutteet, sillä huonosta turvallisuuden tasosta kärsii niin luotettavuus kuin käytettävyyskin. Tärkeäksi menestystekijäksi tulee nousemaan luottamus tietojenkäsittelyä kohtaan (Andreasson ym. 2016, 12.) Tietosuoja on mahdollisuus kehittää yrityksen toimintaa, ei este.

Teknologisen kehityksen ja valtioiden välisen yhteistyön kasvamisen myötä on välttämätöntä luoda uudistuksia. Ihmisistä kerätään jatkuvasti enemmän tietoa, ja tiedonkeruuseen käytettävät menetelmät lisääntyvät. Samanaikaisesti perusoikeuskirjan 8 artiklan 1 kohdan mukaan yksilöllä on täysi oikeus suojata henkilötietonsa (EU 2000/C 364/01). Euroopan unionissa ei ole ennen uutta tietosuoja-asetusta ollut yhtenäistä kantaa tietosuojaan. Uuden asetuksen tarkoituksena on suoraviivaistaa unionin sisäinen käsitys asiasta ja pyrkiä turvaamaan jäsenten oikeus tietosuojaan niin Euroopan sisällä ja sen ulkopuolella. (Andreasson ym. 2016, 12-13.)

Kehityksen kulkua on mahdotonta ennustaa. Ennen uutta lainsäädäntöä, viimeisin voimassa oleva henkilötietodirektiivi astui voimaan vuonna 1995. Tällöin ei ollut olemassa samanlaisia verkkopalveluita kuin nykyään, joten niiden mukanaan tuomia haasteitakaan ei ollut. Euroopan unionin on pidettävä huolta siitä, että ihmisten oikeus tietosuojaan taataan myös sosiaalisen median, pelvipalveluiden, älykorttien ja muiden keksintöjen aikana. (Oikeusministeriö 2015.)

Kuva 2. Uuden tietosuoja-asetuksen keskeiset osa-alueet.
(Vahti 2016, 7)

3 LAINSÄÄDÄNTÖ

Tässä osiossa käydään läpi lainsäädäntöä. Tarkoituksena on selvittää syitä miksi uusi asetus tehtiin ja mitä se tulee muuttamaan vertaamalla uudistuksia vanhoihin, vielä voimassa oleviin säädöksiin. Lisäksi käydään läpi muutoksia niin rekisteröidyn, kuin rekisterinpitäjän kannalta.

3.1 Taustaa

Henkilötietojen käsittelyn mittakaava on kasvanut paljon viime vuosina. EU:n nykyinen, vielä voimassa oleva henkilötietodirektiivi astui voimaan vuonna 1995, jolloin informaation liikkuminen oli suhteessa vähäisempää kuin nykyisin. Henkilötietoja ei myöskään pystytty hyödyntämään samalla tavalla kuin nykyään. (U 21/2012 vp, 1-3)

Kuva 3. Tietosuoja-asetuksen valmistelun vaiheet.
(Rovamo 2016, 4)

Teknologia kehittyy ja esimerkiksi sosiaalinen media, pilvipalvelut sekä nettikaupat ovat luoneet entistä globaalimaan toimintaympäristön. Digitalisoituminen on johtanut henkilötietojen keräämisen kasvamiseen ja niiden hyväksikäyttämiseen muun muassa markkinoinnissa. Käsitys tietosuojasta on muuttunut ja näin ollen

myös eurooppalaisen tietosuojasäätelyn uudistus on paikallaan. Euroopan unionin tavoitteena oli luoda riskilähtöinen ja teknologiariippumaton sääntely, joka ottaisi huomioon teknologian kehityksen ja sen mukanaan tuomien uusien tiedonkeruumenetelmien luomat riskit sekä velvoittaisi mitoittamaan suojausmekanismit edellä mainittujen riskien mukaisesti. (Vahti 2016, 6.)

EU:n uuden tietosuojalainsäädännön taustoja tutkittaessa joudutaan palaamaan vuoteen 2007, jolloin Lissabonin sopimuksessa astui voimaan päätös, jonka mukaan EU:n perusoikeuskirjasta tehtiin oikeudellisesti sitova, eli sille annettiin sama oikeusarvo kuin unionin perussopimuksille. Kyseisen perusoikeuskirjan artiklat 7 ja 8 säätävät jokaiselle oikeuden yksityiselämän ja perhe-elämän, sekä kodin ja viestinnän suojaan (OM2015-00233, 3). Helmikuussa 2009 Eurooppa-neuvosto hyväksyi Tukholma ohjelman (EU 2010/C 115/71), jossa todettiin yksityisyyden suojan olevan turvattu EU:n perusoikeuskirjassa ja tästä johtuen Euroopan neuvoston tulee varmistaa tietosuojasopimuksen periaatteiden toteutumista muun muassa arvioimailla nykyisen tietosuojan tasoa. (Eurooppa-neuvosto 2010, 10-11.)

Euroopan komissio aloitti uuden lainsäädännön valmistelemisen, jonka aikana muun muassa konsultoitiin kansallisista tietoturvaviranomaisista koostuvaa työryhmää ja kysyttiin kansan mielipiteitä eurobarometrikyselyiden avulla. Tammikuussa 2015 komissio antoi ehdotuksen yleisestä tietosuoja-asetuksesta (COM(2012) 11 final), direktiivin henkilötietojen suojasta lainvalvonnassa (COM(2012) 10 final), sekä tiedonannon ”Yksityisyydensuoja verkottuvassa maailmassa” (COM(2012) 9 final), jota tultaisiin käyttämään Euroopan uutena tietosuojakehyksenä. Tiedonannossa todettiin teknologian kehityksen ja globalisaation muuttaneen ihmisten käsitystä tietosuojasta ja kuinka henkilötietojen kerääminen ja käsittely ovat myös muuttuneet. Muutoksen tavoitteena on parantaa yksityishenkilöiden oikeutta valvoa henkilötietojaan sekä parantaa luottamusta online-palveluihin. (OM2015-00233, 2-3.)

Perusteluna uudelle asetukselle esitettiin Euroopan unionin toissijaisuusperiaate. Tämän periaatteen takia päätöksiä tehdään unionin tasolla ainoastaan niissä tilanteissa, joissa jäsenvaltiot eivät pysty itsenäisesti tavoitteitaan saavuttamaan. Valtioiden rajojen yli siirrettävien henkilötietojen määrä on jo niin korkea, että

jäsenvaltioiden välinen yhteinen henkilötietojen suoja katsotaan loogisemmaksi vaihtoehdoksi. Asetusehdotuksessa todetaan, ettei nykyinen henkilötietodirektiivi ole pystynyt parantamaan kuluttajien luottamusta verkkoympäristössä tehtyihin toimintoihin. Uudella ja vahvemmalla säädöksellä pyritään parantamaan niin yksittäisten henkilöiden kuin yritysten luottamusta digitaalisten markkinoiden tulevaisuuteen. (COM(2012) 11 final, 2.)

Maaliskuussa 2014 Euroopan parlamentti hyväksyi tietosuoja-asetusehdon ja asetuksen käsittely siirtyi eteenpäin unionin oikeus- ja sisäasioiden neuvostolle (OSA). Loka- ja joulukuussa 2014 neuvosto keskusteli oikeudesta tulla unohdetuksi ja pääsi sopimukseen asetuksen alueellisista soveltamiseroista, rekisterinpitäjän ja tietojenkäsittelijän velvollisuuksista, sekä tiedonsiirrosta kolmansien maiden osalta. Kesäkuussa 2015 neuvosto pääsi yhteisymmärrykseen ja kolmikantaneuvottelut parlamentin ja neuvoston välillä alkoitettiin. Uusi asetus hyväksyttiin virallisesti vuonna 2016 alkupuolella, josta alkoi kahden vuoden siirtymisaika. Uusi asetus tulee kokonaisuudessaan käytäntöön vuonna 2018. (U 21/2012 vp, 1)

3.2 Lainmukaisuus

Henkilötietolaki määrittelee tietojen käsittelyn lainmukaisuuden (Henkilötietolaki 523/1999, 8§). Määritelmä löytyy käsittelyn yleisten edellytysten alta, joita ovat muun muassa rekisteröidyn suostumus tietojen keräämiseen, toimeksianto, sopimus ja rekisteröidyn elintärkeä etu.

Mikäli käsittelyn yleisiä edellytyksiä ei pystytä täyttämään, ei tietoja voida kerätä. Edellytysten täyttyessä rekisterinpitäjän on kuitenkin otettava huomioon käyttötarkoitussidonnaisuus. Rekisterinpitäjä ei siis ole oikeutettu käsittelemään alkuperäisen tarkoituksen kanssa ristiriidassa olevia tietoja (Vanto 2011, 44). Rekisteröidyn suostumusta tietojen keräämiseen käsitellään aina tapauskohtaisesti, eikä henkilötietojen käsitteleminen ole sallittua ilman rekisteröidyn suostumusta. Rekisteröidylle täytyy tehdä yksiselitteinen ja selkeä selvitys henkilötietojen keräämisen syistä, jonka jälkeen hän päättää allekirjoittaako suostumuksen. Mikäli sairaalaan saapuneelta rekisteröidyltä

pyydetään yleistä suostumusta henkilötietojen luovuttamiseen, ei tämä ole lain puitteissa riittävän yksiselitteistä, sillä rekisteröity ei voi tietää mitä tietoja tämä voi myöhemmin koskea. (Vanto 2011, 44-45.)

Rekisteröity voi allekirjoittaa sopimuksen tai antaa toimeksiannon, jotka oikeuttavat henkilötietojen käsittelyn. Henkilötietojen käsittely on myös sallittua, jos se tapahtuu rekisteröidyn elintärkeän edun pohjalta. Esimerkiksi tilanteessa, jossa rekisteröity on vakavasti loukkaantunut onnettomuudessa, voidaan henkilötietoja käsittelemällä ottaa selvää nimistä ja puhelinnumeroista. Arkaluontoisten, kuten terveyteen liittyvien tietojen käsittely on kuitenkin kiellettyä ilman rekisteröidyn suostumusta. Poikkeuksena tähän mainittakoon kuitenkin tilanne, jossa rekisteröity on esimerkiksi tajuton, eikä siis pysty antamaan suostumustaan. Tällaisissa tilanteissa voidaan arkaluontoisiakin henkilötietoja käsitellä ilman rekisteröidyn suostumusta, jos siitä on hänelle elintärkeää etua. (Vanto 2011, 46-47.)

Laki sekä laissa säädetty tehtävä tai velvoite voivat oikeuttaa henkilötietojen käsittelemiseen, mutta käsittelyä ei voida perustella asetuksella (Henkilötietolaki 523/1999, 8§). Lait toimivat oikeudellisen sääntelyn pohjana, kun taas asetukset ovat lakia tai sen tiettyä kohtaa täydentäviä tai tarkentavia osia. Laki määrittelee yksityisyyden suojan työelämässä. Kyseinen laki antaa työnantajalle luvan käsitellä työntekijöidensä henkilötietoja. Rekisterinpitäjä saa käsitellä rekisteröidyn henkilötietoja, jos heillä on esimerkiksi asiakas- tai palvelusuhde. Rekisterinpitäjä on kuitenkin velvollinen perustelemaan henkilötietojen käsittelyn.

Kuten jo edellä mainittiin, on yritysten sisällä tapahtuva henkilötietojen käsittely sallittua. Oikeus tietojen käsittelyyn koskee kuitenkin vain rekisteröityjä, joilla on asiallinen kytkös johonkin yrityksen osaan (Vanto 2011, 49). Henkilötietoja saa käsitellä, jos käsittelyyn liittyy henkilön asemaan, tehtävään tai niiden hoitoon liittyvä julkinen tieto. Tietojen tulee kuitenkin turvata rekisterinpitäjän tai sivullisen tietojen saajan oikeudet, jotta elinkeinoelämässä luottotietojen käsittely olisi mahdollista (Vanto 2011, 50). Tietosuojalautakunta voi myöntää poikkeusluvan henkilötietojen käsittelyyn. Lupaa voidaan hakea, jos käsittelylle ei löydy muita edellytyksiä. Poikkeusluvalla myönnetty tietojen käsittely ei saa rikkoa yksityisyyden suojaa. (Vanto 2011, 51-52.)

Henkilötietojen tarkastelun lainmukaisuutta tutkittaessa termit tarpeellisuusvaatimus ja virheettömyysvaatimus tulevat useasti esille. Tarpeellisuusvaatimuksen tarkoituksena on rajoittaa henkilötietojen käsittely vain tarkoituksen kannalta tärkeälle alueelle. Otetaan esimerkkinä tavarantoimittaja. Rekisteröity tilaa jotain verkkokaupasta. Tavarantoimittajan kannalta tärkeitä henkilötietoja ovat tässä tapauksessa rekisteröidyn nimi, puhelinnumero ja osoite. Tavarantoimittaja ei kuitenkaan tarvitse tietoja rekisteröidyn vuosituloista. Tarpeettomia tietoja ei tule käsitellä. Virheettömyysvaatimuksen tarkoituksena on velvoittaa rekisterinpitäjää huolehtimaan tietojen virheettömyydestä ja ajantasaisuudesta. (Vanto 2011, 53.)

Tiivistettynä henkilötietojen käsittely on lainmukaista, kun rekisteröity antaa suostumuksensa tietojen käsittelyyn ja pohjaa päätöksensä selkeään selvitykseen, jonka hän on ymmärtänyt. Rekisteröidylle tulee myös ilmoittaa oikeudesta peruuttaa suostumus tietojen keräämiseen. Tietosuojalainsäädäntö tuo uudistuksena määritelmän, jonka mukaan käsittely on lainmukaista, jos se on tarpeen niin rekisteröidyn, kuin toisen luonnollisen henkilön elintärkeän edun suojaamiseksi. Muina uudistuksena tulevat yleistä etua koskevan tehtävän suorittaminen, julkisen vallan käyttö sekä kolmannen osapuolen tai rekisterinpitäjän oikeuksien toteuttaminen. (EU 2016/679, 36-37.)

3.3 Arkaluontoisten tietojen käsittely

Arkaluontoisten tietojen käsittely on henkilötietolaissa kielletty ilman rekisteröidyn siihen antamaa suostumusta tai muuta henkilötietolaista löytyvää poikkeusta (Henkilötietolaki 523/1999, 3 luku, 12§). Arkaluontoisiksi henkilötietolaki määrittää tiedot, jotka on tarkoitettu kuvaamaan rotua tai etnistä alkuperää; henkilön yhteiskunnallista, poliittista tai uskonnolista vakaumusta tai ammattiliittoon kuulumista; rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta; henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia; henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka henkilön sosiaalihuollon tarvetta tai

hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia (Henkilötietolaki 523/1999, luku 3, 11§).

Arkaluontoisten henkilötietojen käsittely käytännössä tarkoittaisi esimerkiksi internetissä tapahtuvaa mainontaa, joka pohjautuu rekisteröidyn seksuaaliseen suuntautumiseen. Toinen esimerkki on kauppaketjuissa kanta-asiakastietojen käsittely, jos esimerkiksi asiakastiedoista selviäisi rekisteröidyn alkoholinkulutustottumukset. Tällöin asiakastiedoista voidaan päätellä rekisteröidyn alkoholiongelma, joka liittyy hänen terveyteensä ja on täten arkaluontoinen asia. (Vanto 2011, 57.)

Rekisteröidyn suostumuksen laatu arkaluontoisten asioiden käsittelyyn on myös tarkkaan määritelty. Rekisterinpitäjän tulee pystyä todistamaan, että rekisteröity on hyväksynyt tietojen käsittelyn ehdot ja ymmärtänyt ne. Suostumuksen tulee siis olla nimenomainen. Tällä termillä tarkoitetaan, että rekisteröity sanoo hyväksyvänsä tai rastittaa itse kohdan, jolla hän kertoo hyväksyvänsä arkaluontoisten tietojen käsittelyn. Suostumukseksi ei riitä valmiiksi rastitettu ruutu, josta rekisteröidyn tulisi itse ottaa merkki pois, mikäli ei halua tietojaan käsiteltävän. Suostumuksen tulee olla kirjallinen ja yksilöllisesti laadittu. Tietoja voidaan käsitellä ilman suostumusta, mikäli rekisteröity on tuonut ne itse julkisuuteen, tai jos tietojen käsittelystä on rekisteröidylle tai toiselle henkilölle elintärkeää etua eikä rekisteröity pysty jostain syystä antamaan suostumustaan. Käytännön esimerkkinä tästä on ensiaputilanne. (Vanto 2011, 58-60.)

Muita poikkeuksia arkaluontoisten tietojen käsittelyyn on luotu helpottamaan eri yhdistysten ja työpaikkojen toimintaa. Esimerkiksi kirkko saa käsitellä henkilön uskontoon tai yhteiskunnalliseen vakaumukseen liittyviä tietoja, kunhan käsittely pysyy kirkon sisäisenä. Myös työnantajalla on oikeus käsitellä joitain arkaluontoisia tietoja, jos ne ovat työoikeudellisesti relevantteja. (Vanto 2011, 60-62.)

Uusi tietosuoja-asetus käsittelee arkaluontoisten asioiden käsittelyn lähes samalla tavoin kuin henkilötietolaki. Uutena osiona tulevat erityisten henkilötietoryhmien käsittelyssä tarvittavat asetukset. Näitä ovat jo henkilötietolaissa määriteltyjen tietojen lisäksi henkilöiden geneettiset ja biometriset tiedot. Lisäksi uusi asetus tuo mukanaan oikeuden erityisten tietoryhmien käsittelyyn, mikäli se katsotaan

tarpeelliseksi sosiaaliturvan, työoikeuden tai sosiaalisen suojelun kannalta. Tämä poikkeus asetettiin, jotta rekisterinpitäjän ja rekisteröidyn oikeudet ja velvoitteet pystyttäisiin toteuttamaan. Toisena poikkeuksena tulee tietojen käsittelyn sallittavuus sen ollessa tarpeen kansanterveydellisistä syistä. Tällaisia tilanteita ovat esimerkiksi epidemian leviämisestä johtuva tietojen käsittely, jotta voitaisiin taata turvallisuusnormiston toteutuminen ja yleisten terveysriskien hallinta. (EU 2016/679, 38-39.)

3.4 Rekisteröidyn oikeudet

Tässä osiossa käydään läpi uuden tietosuoja-asetuksen asettamia rekisteröidyn oikeuksia, ongelmia joita uusista oikeuksista löydettiin sekä rekisteröidyn oikeussuojakeinoja.

3.4.1 Läpinäkyvyys ja tiedonsaantioikeus

Ennen uutta tietosuoja-asetusta, läpinäkyvyyden käsitettä ei oltu Euroopan unionin laissa määritelty. Vuonna 2012 tietosuoja-asetuksen artikla 11 toi mukanaan kuitenkin pakotteen, jonka varjolla rekisterinpitäjän täytyy tarjota selkeää ja helposti saatavilla olevaa tietoa tietosuojastandardeista. (COM(2012) 11 final, 49.)

Vuonna 2016 julkaitussa tietosuoja-asetuksessa rekisterinpitäjälle määrätään myös muita pakotteita tiedonsaantiin liittyen. Rekisterinpitäjä on vastuussa ilmoittaa palvelua käyttävälle henkilölle tiedot rekisterinpitäjän ja tämän edustajan henkilöllisyyksistä yhteystietoineen, sekä myös tietosuojavastaavan yhteystiedot. Rekisteröityneelle henkilölle on ilmoitettava perusteet henkilötietojen keräämiseen ja niiden säilytysaika. Rekisteröidylle on myös ilmoitettava hänen oikeuksistaan, kuten mahdollisuudesta vaatia rekisterinpitäjää poistamaan henkilötietoja tai vastustaa niiden käsittelyä. (COM(2012) 11 final, 50.)

Rekisteröidyllä on oikeus päästä käsiksi omiin henkilötietoihinsa, joten rekisterinpitäjän täytyy pystyä tarjoamaan etäpääsy suojattuun järjestelmään, josta

rekisteröity saa suoran pääsyn henkilötietoihinsa. Rekisteröidyn pääsy järjestelmään täytyy olla mahdollisimman vaivaton. (EU 2016/679, 12.)

Rekisteröityneellä on myös valitusoikeus. Valitusta tehdessään vastuu valitusoikeuden ilmoittamisesta valvontaviranomaiselle on rekisteröityneellä. Valituksen mukana tulee ilmoittaa henkilötietojen vastaanottajat, tieto siirretäänkö henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, sekä muut rekisteröidyn kannalta tarpeelliset tiedot asianmukaisen tietojenkäsittelyn takaamiseksi. (COM(2012) 11 final, 50-51.)

Tietoja kerätessä on rekisteröidylle ilmoitettava tietojen luovuttamisen vapaaehtoisuudesta sekä seurauksista, jos tietojen luovuttamista ei hyväksytä. Jos tietoja kerätään muista lähteistä kuin rekisteröidyltä, on ilmoitettava, mistä tiedot on saatu. Edellä mainitut tiedot on toimitettava rekisteröidylle henkilötietoja tallentaessa tai kohtuullisen ajan kuluessa keräämisestä. (EU 2016/679, 40-41.)

Mikäli rekisteröity on jo aiemmin saanut tiedot siitä, että hän on luovuttamassa henkilötietojaan tai luovuttamisesta koituu kohtuutonta vaivaa niiden kerääjälle, esimerkiksi muiden henkilötietojen karsimisen vuoksi, ei rekisteröidylle tarvitse toimittaa tietoa keräämisestä. Rekisteröidyllä on myös oikeus peruuttaa suostumuksensa henkilötietojen keräämiseen. Tämä ei kuitenkaan muuta jo kerättyjen henkilötietojen lainmukaisuutta. (EU 2016/679, 40-41.)

Henkilötietodirektiivin 10. artiklaan verrattuna uusi tietosuoja-asetuksen 14. artikla tuo lisänä rekisterinpitäjän velvollisuuden ilmoittaa tietojen säilytysajan ja lähteen. Lisänä tulee myös rekisteröidyn oikeus pyytää oikaisua tai tietojen poistamista. (EU 2016/679, 40-41; EU 95/46/EY, 41.)

3.4.2 Uudet oikeudet

Uusi tietosuoja-asetus toi mukanaan useita muutoksi ja päivityksi, joista tärkeimpiä ovat rekisteröidyn oikeus tulla unohdetuksi ja oikeus vaatia tietojen siirtoa ja tietojen käsittelyn rajoittamista. Rekisteröitynyt voi myös vaatia tietojensa poistamista kokonaan, jolloin rekisterinpitäjän tulee poistaa henkilötiedot mahdollisimman pian. Perusteluina henkilötietojen poistamiseen voi vedota

tietojen keräämisen tarkoituksen muutokseen, jolloin tiedot eivät olisi tarpeellisia tai tiedon käsittely ei ole lainmukaista. Esimerkki tietojenkeruun tarkoituksen muutoksesta voi olla tapaus, jossa tietojen kerääjä ilmoittaa keräävänsä verkkokaupassa käyvien henkilöiden lukumäärää mutta muuttaa myöhemmin tiedonkeruun laadun koskemaan tuotetyyppejä, joita palvelun käyttäjät selaavat. Myös rekisteröidyn päätös muuttaa suostumustaan henkilötietojen keräämiseen on syy poistaa henkilötiedot. Jos saadut henkilötiedot on kerätty palveluntarjonnan yhteydessä, on ne poistettava. (EU 2016/679, 43-44.)

3.4.3 Ongelmat

Muutokset tuovat kuitenkin aina mukanaan ongelmia. Erityisesti uusien tietosuoja-asetusten soveltaminen tuotti päänvaivaa. Esimerkiksi vuonna 2014 Euroopan tuomioistuin päätti, että ihmiset voivat vaatia heidän nimellään löytyvien hakukonetulosten piilottamista, mikäli niiden perusteella löytyvät tiedot ovat todistettavasti virheellisiä. Vuonna 2016 Ranskan tietosuojavaltuutettu antoi Googlelle sakot ja perusteli tätä väittäen, että Google ei ollut noudattanut 2014 voimaan astunutta säädöstä. Googlen vasta-argumentti oli, että he ovat noudattaneet kaikkia vaatimuksia, sillä Euroopan sisälle luodut hakukoneet, kuten Google.fr ja Google.fi eivät enää näytä poistettuja henkilötietoja, mutta maailmanlaajuiseksi luotu Google.com ei ole velvollinen noudattamaan Euroopan sisäisiä asetuksia. Googlen lakiasiainjohtaja Kent Walkerin mukaan Google noudattaa niiden maiden lakeja, joissa he toimivat, mutta ongelmallista on se, että Ranska ulottaa lakinsa globaaliksi. (Tivi 2016.)

Suurin ongelma on siis siinä, kuinka pitkälle voidaan uutta tietosuojalaki soveltaa. Voiko Euroopan Unionin asetus vaikuttaa yli maiden rajojen? Voidaanko siis olettaa, että rikoksentekijällä on oikeus tulla unohdetuksi työpaikan omissa rekistereissä rikoksen vanhennuttua?

Rekisteröity henkilö voi vaatia henkilötietojensa käsittelyn rajoittamista kiistämällä tietojen oikeellisuuden. Henkilötietojen käsittelyä tulee tällöin rajoittaa siihen asti, kunnes rekisterinpitäjä tarkastastaa tietojen paikkaansa pitävyyden. Rekisterinpitäjän on ilmoitettava kaikille asian osapuolille mahdollisista tietojen

muutoksista, poistoista tai rajoituksista. Rekistreöidylle kuuluu myös oikeus siirtää tietojaan. Tiedot tulee antaa rekisteröidylle sähköisessä muodossa, jonka jälkeen rekisteröity voi siirtää ne toiselle rekisterinpitäjälle. Rekisteröidyllä on oikeus siirtää tietoja, jos hän on itse suostunut tietojenkäsittelyyn tai käsittely on automatisoitua. (EU 2016/679, 45-46.)

3.4.4 Oikeus vastustaa henkilötietojen käsittelyä ja profilointia

Rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä, jos käsittelystä mahdollisesti aiheutuu haittaa rekisteröidyn oikeuksia kohtaan. Mikäli tietojen kerääminen ja käsittly koskee suoramarkkinointia, on rekisteröidylle tarjottava mahdollisuus vastustaa henkilötietojen käsittelyä erillään muusta tiedotuksesta. Näistä kohdista päätettiin ensimmäistä kertaa asetuksen vuonna 2012 julkaistussa versiossa. (COM(2012) 11 final, 55.)

Henkilötietodirektiivissä rekisteröidylle annettiin oikeus vastustaa henkilötietojensa käsittelyä, jos käsittely koskee yleistä etua tavoittelevan tehtävän suorittamista tai tietoja käsitellään rekisterinpitäjän tai ulkopuolisen intressien toteuttamiseksi. Henkilötietodirektiivi ei mainitse erikseen mitään, mikä koskisi suoramarkkinointia. (EU 95/46/EY, 42-43.)

Uutena tietosuoja-asetus tuo mukanaan rekisteröidyn oikeuden vastustaa profilointia. Tällä tarkoitetaan, että luonnollisen henkilön ei tarvitse joutua toimenpiteen kohteeksi, josta hänelle voi seurata oikeudellisia vaatimuksia. Luonnollisen henkilön ei myöskään tarvitse joutua prosessin kohteeksi, jossa häntä kategorisoidaan ainoastaan automaattisen tietojenkäsittelyn avulla, esimerkiksi terveyden tai taloudellisen tilanteen arvioimista varten. Profilointia voidaan suorittaa ainoastaan tilanteissa, joissa rekisteröity on tehnyt tietojen käsittelijän kanssa sopimuksen, antanut suostumuksensa tai profilointi on kyseisessä tapauksessa hyväksytty unionin tai jäsenvaltion laissa. (COM(2012) 11 final, 55-56.)

Mikäli valvontaviranomaisen päätökseen ei olla tyytyväisiä, voi valituksen tehnyt yhdistys, henkilö tai ulkopuolinen oikeushenkilö valittaa päätöksestä

tuomioistuimeen. Valituksen voi tehdä ainoastaan sen maan tuomioistuimelle, jossa päätöksen tehnyt valvontaviranomainen työskentelee. Mikäli päätöksen tehnyt valvontaviranomainen toimii jossain muussa maassa kuin rekisteröity itse, on rekisteröidyllä oikeus pyytää oman asuinvaltionsa valvontaviranomaista aloittamaan oikeuskäsittelyn päätöksen tehnyttä valvontaviranomaista vastaan. Niin tietosuoja-asetus kuin henkilötietodirektiivi antavat mahdollisuuden valittaa valvontaviranomaisen tekemästä päätöksestä. (EU 95/46/EY, 47; COM(2012) 11 final, 92.)

Tietosuoja-asetus ja henkilötietodirektiivi antavat rekisteröidylle myös oikeuden nostaa kanteen. Kanne on nostettava tuomioistuimessa henkilötietojen käsittelijää tai rekisterinpitäjää kohtaan. Kanteen nostamisen voi perustella epäilyllä rekisteröidyn oikeuksien rikkomisesta. Kanne on nostettava rekisterinpitäjän tai tietojenkäsittelijän toimivaltiossa tai rekisteröidyn asuinvaltiossa. Poikkeuksena tähän on, jos rekisterinpitäjä on viranomainen, jonka toiminta pohjautuu julkisen vallan käyttöön. Tällaisissa tilanteissa kanne on nostettava siinä maassa, missä viranomainen työskentelee. (EU 95/46/EY, 45; COM(2012) 11 final, 92.)

3.4.5 Oikeussuojakeinot

Henkilötietodirektiivi ja tietosuoja-asetus molemmat määrittelevät rekisteröidylle oikeuden valittaa henkilötietojen käsittelyssä potentiaalisesti tapahtuneista rikkeistä. Valituksen voi tehdä myös yhdistys, joka on perustettu henkiötietojen suojaan liittyvien oikeuksien suojelemiseen. Valituksen voi tehdä minkä tahansa jäsenvaltion valvontaviranomaiselle. (EU 95/46/EY, 48; COM(2012) 11 final, 91-92.)

3.5 Rekisterinpitäjän velvollisuudet

Uuden tietosuoja-asetuksen mukana myös rekisterinpitäjän velvollisuudet kasvavat. Tietojen suojaamisesta pyritään tekemään oletusarvoista, niin olemassa olevissa palveluissa ja ohjelmistoissa kuin uusien suunnittelussakin. Uutena velvollisuutena rekisterinpitäjälle tulee vaikutusten arviointi, jonka tarvittavuus

määritetään tapauskohtaisesti. Lainsäädäntöön tulee myös muutoksia. Muun muassa velvollisuus ilmoittaa tietovuodoista laajenee, ja tietosuojarikkeistä seuraa rangaistus. Lisäksi henkilötietojen käsittelijän vastuu kasvaa. Uusi asetus määrittelee myös tilanteita, joissa rekisterinpitäjän täytyy nimittää tietosuojavastaava, jonka tehtävänä on valvoa ja neuvoa asetusten noudattamista. (EU 2016/679, 47-54.)

3.5.1 Yleiset velvollisuudet

Rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuoja-asetusta. Osoittaakseen noudattavansa asetusta rekisterinpitäjän täytyy toteuttaa ennalta määritetyt toimenpiteet. Nämä toimenpiteet ottavat huomioon käsittelyn tarkoituksen ja laajuuden, riskien todennäköisyyden, vakavuuden ja käsittelun luonteen. Rekisterinpitäjän on myös oltava varma, että tietojenkäsittely koskee vain tarkoituksen kannalta oleellisia henkilötietoja. (EU 2016/679, 47-48.)

Rekisterinpitäjällä on vastuu pitää kirjaa käsittelyn kulusta. Ylös tulee kirjata rekisterinpitäjän, tietosuojavastaavan sekä rekisterinpitäjän edustajan yhteystiedot. Muita kirjattavaksi vaadituuja tietoja ovat tiedot henkilötietojen siirtämisestä, tietojen säilytysajat, käsittelyn tarkoitus sekä kuvaus käytettävistä turvatoimista. Turvatoimina rekisterinpitäjän tulee pitää huolta järjestelmä luottamuksellisuudesta. Tietojen tulee olla aina käytettävissä ja järjestelmän tulee olla vikasietoinen. Rekisterinpitäjän on varauduttava järjestelmävian sattuessa tarjoamaan toinen luotettava reitti. Valvontaviranomaisella on oikeus saada kirjallinen versio selosteesta, mikäli hän sitä pyytää. Selostetta ei tarvitse tehdä, mikäli organisaatiossa on alle 250 työntekijää. Poikkeuksena tähän ovat tilanteet, joissa rekisteröidyn oikeuksille ja vapauksille koetaan aiheutuvan haittaa. (EU 2016/679, 50-52.)

Rekisterinpitäjälle uutena asetuksena tulee vastuu ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle 72 tunnin sisällä loukkauksen havaitsemisesta. Mahdollisten viivästysten sattuessa tulee rekisterinpitäjän toimittaa valvontaviranomaiselle selvitys, jossa hän selittää viivästymisen syyt. Selvitykset arvioidaan tapauskohtaisesti. Ilmoitusta ei kuitenkaan tarvitse toimittaa,

mikäli tietoturvaloukkauksen seurauksena ei synny rekisteröidyn oikeuksiin kohdistuvia riskejä. Henkilötietojen käsittelijän tulee toimittaa rekisterinpitäjälle selvitys tietoturvaloukkauksista. Selvitykseen tulee kirjata kuvaus loukkauksesta, loukkauksen kohteeksi joutuneiden ryhmien tai henkilöiden määrä, tietosuojavastaavan yhteystiedot sekä rekisterinpitäjän ehdottamat tai jo toteuttamat toimenpiteet loukkauksen ja sen haittavaikutusten suhteen. Rekisterinpitäjän vastuulla on myös kaikkien loukkausten dokumentointi. Dokumentoinnista tulee käydä ilmi loukkauksesta johtuvat toimenpiteet ja niiden vaikutukset. Dokumentoinnin tarkoituksena on luoda aineistoa, josta voidaan tarkastaan onko tietosuoja-asetusta noudatettu. (EU 2016/679, 52.)

Tietoturvaloukkauksen sattuessa tulee siitä ilmoittaa rekisteröidyille välittömästi, mikäli heidän oikeuksilleen koetaan koituvan mahdollisia riskejä. Rekisteröidyllä on oikeus saada samat tiedot kuin tietosuojaviranomaisella. Mikäli rekisterinpitäjä on toteuttanut asiaan kuuluvat suojatoimet, kuten pitänyt huolta siitä, että tietoturvaloukkauksen tekijät eivät pysty tunnistamaan rekisteröityjä henkilöitä tiedoista, ei rekisteröidylle tarvitse ilmoitusta tietoturvaloukkauksesta tehdä. Rekisteröidylle ei myöskäänn tarvitse ilmoittaa, jos voidaan todetä, että riski ei todennäköisesti enää toistu. Valvontaviranomainen voi kehottaa rekisterinpitäjää tekemään ilmoituksen rekisteröidylle, mikäli tämä ei ole sitä jo tehnyt. (EU 2016/679, 52-53.)

Mikäli koetaan, että henkilötietojen käsittelyyn kohdistuu normaalia suurempi riski, tulee rekisterinpitäjän tehdä käsittelytoimien vaikutuksista arviointi. Rekisterinpitäjän tulee konsultoida tietosuojavastaavaa, mikäli tällainen on nimitetty. Erityisesti vaikutustenarviointi on tärkeä tehdä tilanteissa, joissa päätöksiä tehdään automaattisen käsittelyn pohjalta. Tällaisia ovat esimerkiksi profiloinnin perustella tehdyt päätökset, joissa henkilöön kohdistuu oikeusvaikutuksia. Vaikutustenarviointi on tarpeellista myös henkilötietojen käsittelyjäissä jotka, ovat laajamittaisia ja kohdistuvat rikkomuksiin liittyviin tietoihin. (EU 2016/679, 53-54.)

3.5.2 Tietosuoja ja käsittelyn turvallisuus

Vuonna 2012 Euroopan parlamentti ja neuvosto julkisti ehdotuksen asetuksesta, jonka mukaan tietosuojasta ja tietoturvasta tehtäisiin oletusarvoista. Tällä tarkoitetaan, että tietosuoja- sekä tietoturvavaatimukset otetaan huomioon tuotteiden ja palveluiden suunnitteluvaiheessa. Rekisterinpitäjän tulee käyttää asianmukaisia toimenpiteitä ja uusinta tekniikkaa varmistaakseen asetuksen noudattamisen. Rekisterinpitäjän tulee varmistaa, että kerätyistä henkilötiedoista käsitellään ainoastaan tarkoituksen kannalta välttämättömät eikä tietoja säilytetä kauempaa kuin on tarvetta. (COM(2012) 11 final, 58.)

Kuva 4. Henkilötietojen elinkaari.
(Vahti 2016, 24)

Rekisterinpitäjän tulee yhteistyössä tietojen käsittelijän kanssa varmistaa henkilötietojen asianmukainen turvallisuus. Tietojen turvallisuudesta tulee tehdä riskiarviointi, jossa turvatoimenpiteille arvioidaan kustannukset. Riskejä arvioidessa on otettava huomioon uusimpien tekniikoiden mukanaan tuomat riskit. Henkilötiedot on pystyttävä suojaamaan ulkoisilta muutoksilta, poistamiselta tai muulta häviämiseltä, tietojen luvattomalta levittämiseltä sekä lainvastaiselta käsittelyltä. (COM(2012) 11 final, 62.)

Henkilötietodirektiivi asettaa rekisterinpitäjälle vastuun käsittelyn turvallisuuden vastaamisesta. Rekisterinpitäjä voi siirtää henkilötietojen käsittelyn ulkopuoliselle taholle, mutta on silti vastuussa turvatoimien takaamisesta. (Henkilötietolaki 523/1999.)

Uutena tietosuoja-asetus tuo lainsäädännöllisen muutoksen tietosuojan sekä tietoturvan vastuun jakamiseen. Ennen asetusta ainoastaan rekisterinpitäjä on

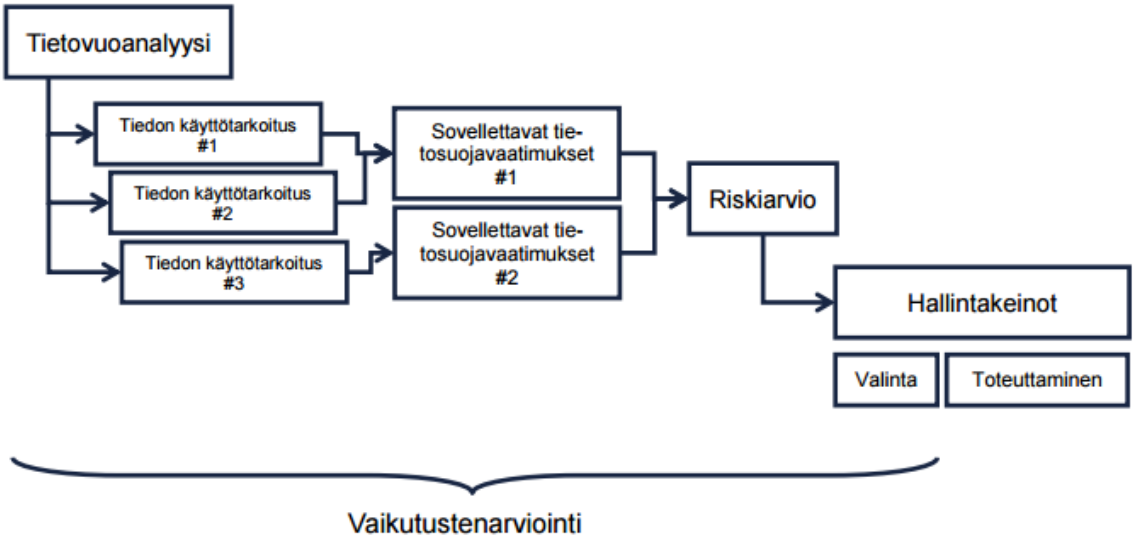
ollut vastuussa tietojen turvallisuuden takaamisesta. Uudessa asetuksessa myös tietojen käsittelijälle asetetaan vastuu. (COM(2012) 11 final, 63-64.)

3.5.3 Vaikutustenarviointi ja ennakkohyväksyntä

Tietosuoja-asetus vaatii rekisterinpitäjää tai henkilötietojen käsittelijää laatimaan arvion henkilötietojen käsittelyn vaikutuksista henkilötietojen suojalle. Arvio tehdään, mikäli tietojen käsittelystä voi niiden laajuuden tai tarkoituksen vuoksi koitua haittaa rekisteröityneen oikeuksiin tai vapauksiin. Riskejä sisältäviä toimenpiteitä ovat esimerkiksi tapaukset, joissa käsitellään yksittäisen henkilön rotua tai terveyttä. Muita vaikutustenarvioinnin vaativia toimenpiteitä ovat julkisesti avoimien alueiden valvonta, sekä suuressa mittakaavassa tapahtuva lasten tietojen käsittely. (COM(2012) 11 final, 64.)

Vaikutustenarvioinnin tulee sisältää sunnitelma käsittelytoimista, arvio sen aiheuttamista riskeistä rekisteröidyn oikeuksiin ja vapauksiin, toimenpiteet ja takaus henkilötietojen suojan varmistamiseksi. Vaikutustenarvioinnista voidaan kuitenkin poiketa, mikäli henkilötietojen käsittely pohjautuu lakisääteiseen velvoitteeseen ja rekisterinpitäjänä toimii viranomainen tai jokin muu julkishallinnollinen taho. (COM(2012) 11 final, 64-65.)

Vaikutustenarvioinnin tarkoitus on korvata henkilötietodirektiivissä säädetty rekisterinpitäjän tai tämän edustajan velvollisuus ilmoittaa valvontaviranomaiselle henkilötietojen käsittelyn alkamisesta. Kyseinen asetus on tiukka, eikä siitä voida poiketa kuin tilanteissa, joissa käsittelytoimet ja käsiteltävät tiedot eivät loukkaa rekisteröidyn oikeuksia ja jäsenvaltiot ovat määrittäneet kaikki kyseiseen tietojenkäsittelyyn liittyvät kriteerit. Vaikutustenarvioinnin takia ei myöskään julkisesta rekisteristä tarvitse tehdä ilmoitusta. (EU 95/46/EY, 43-44.)



Kuva 5. Vaikutustenarviointi
(Vahti 2016, 23)

Mikäli rekisterinpitäjä ei pysty takaamaan henkilötiedoille asianmukaisia suojatoimia, esimerkiksi siirrettäessä tietoa kolmanteen maahan, tulee henkilötietojen käsittelystä saada ennakkohyväksyntä ennen käsittelyn aloittamista. Jos vaikutuksenarvioinnista käy ilmi merkittäviä riskejä henkilötietojen käsittelyyn liittyen, tulee rekisterinpitäjän tai tietojen käsittelijän kuulla valvontaviranomaista ennen käsittelyn aloittamista, jotta rekisteröidyn oikeudet saadaan täytettyä mahdollisimman hyvin. Jos valvontaviranomainen toteaa, ettei käsittely ole asetuksen mukaista, tulee hänen kieltää käsittely ja esittää ehdotuksia puutteiden korjaamiseksi. (COM(2012) 11 final, 65-66.)

3.5.4 Tietosuojavaltuutettu

Suomessa on vain yksi tietosuojavaltuutettu, Reijo Aarnio, joka on tominut tehtävässä vuodesta 1997 lähtien. Valtionneuvosto nimittää tietosuojavaltuutetun määräajaksi ja enintään viideksi vuodeksi. Aarnion viimeinen viiden vuoden toimikausi alkoi marraskuussa 2012. Euroopan tietosuojavaltuutettuna toimii italialaissyntyinen Giovani Buttarelli. Hänen kautensa päättyy vuonna 2019. Tietosuojavaltuutetulta vaaditaan oikeustieteenkandidaatin tutkintoa, vahvaa tietämystä tietosuoja-asioista sekä johtamiskykyä. Tietosuojavaltuutetun tehtävät luetellaan henkilötietolaissa ja laissa tietosuojakunnasta ja tietosuojavaltuutetusta.

Tietosuojavaltuutetun tehtäviin kuuluu esimerkiksi henkilötietojen käsittelyyn liittyvien asioiden ratkaisu ja tietojenkäsittelyn kehityksen seuraaminen ja sen mukaan tarpeellisten lakialoitteiden tekeminen. Tietosuojavaltuutetut ovat tämän lisäksi vastuussa alansa tiedotustoiminnan ylläpitämisestä ja kansainvälisistä yhteyksistä. (Andreasson, Koivisto, Ylipartanen 2013, 15.)

3.5.5 Tietosuojavastaava

Ennen uutta tietosuoja-asetusta, tietosuojavastaavan tehtävät olivat pakollisia ainoastaan sosiaali- ja terveysalalla. Uuden asetuksen myötä muillakin aloilla vaaditaan nimitettäväksi tietosuojavastaava. Tietosuojavastaavan tehtäviin kuuluu tietosuoja-asioista huolehtiminen sekä rekisterinpitäjän apuna ja asiantuntijana toimiminen. Vastaava on myös mukana suunnittelemassa ja toimeenpanemassa yrityksen tietosuoja-asioita. Tietosuojavastaava ei nimestä huolimatta ole kuitenkaan vastuussa tietosuojasta. On tärkeää, että vastaava on tietoinen yrityksestä ja sen käytännöistä, jotta hän voi parhaansa mukaan auttaa rekisterinpitäjää. Tarpeen vaatiessa tietosuojavastaavan tulee kouluttautua pidemmälle. Tietosuojavastaavalle ei suoranaisesti määritellä laissa vaatimuksia, mutta tehtävää hakevalta vaaditaan ”sopivaa koulutusta”. Vastaavalle tulee antaa mahdollisuus raportoida suoraan johdolle ja osallistua asiakaspalveluprosessin kehittämiseen. (Andreasson ym. 2013, 16-18.)

Tietosuojavastaavan nimitys on pakollista, mikäli käsittelyä ei ole suorittamassa viranomainen, tuomioistuin tai julkishallinto. Toinen pakottava tekijä on organisaation ydintehtävien muodostuminen henkilötietojen käsittelytoimista, jotka vaativat henkilöryhmien laajamittaista seurantaa. Konsernin sisällä rittää yhden tietosuojavastaavan nimittäminen olettaen, että häneen saa helposti yhteyden kaikista toimipisteistä. Vastaavaksi nimitetty henkilö voi olla konsernin sisältä tai täysin ulkopuolinen toimija, joka on tietoinen tai on saaanut perehdytyksen yrityksen tietosuoja-asioihin. Vastaavan yhteystiedot tulee ilmoittaa valvontaviranomaiselle. (EU 2016/679, 54-55.)

Tietosuojavastaava on otettava mukaan kaikkiin henkilötietojen suojaa koskevien asioiden käsittelyyn. Rekisterinpitäjän on varmistettava vastaavan pääsy

henkilötietoihin ja olla käytettävissä, jotta vastaava voi suorittaa tehtävänsä. Rekisterinpitäjän tulee myös pitää huolta siitä, että tietosuojavastaava ei ota vastaan ohjeita ulkopuolisilta tehtäviä suorittaessaan. Tietosuojavastaava on salassapitovelvollinen. Vastaavan tehtävät eivät estä yrityksen muissa tehtävissä toimimista, kunhan tehtävät eivät ole ristiriidassa keskenään. (EU 2016/679, 55.)

Jokainen EU:n jäsenvaltio on velvollinen nimittämään ainakin yhden riippumattoman valvontaviranomaisen, jonka tehtävänä on huolehtia uuden asetuksen noudattamista. Hänen tehtäviinsä kuuluu myös huolehtia, että yksityishenkilöiden oikeudet ja vapaudet on turvattu. Valvontaviranomainen ei saa ottaa ulkopuolisia vaikutteita tehtäviä hoitaessaan. Jäsenvaltioilla on vastuu huolehtia, että valvontaviranomaisella on käytettävissään kaikki tämän tarvitsemat resurssit. (EU 2016/679, 65-66.)

Rekisteröidyllä on valitusoikeus siinä maassa, jossa henkilö asuu tai työskentelee tai maassa, jossa vääryys on tapahtunut. Valitus tulee tehdä valvontaviranomaiselle. Valvontaviranomaisen tekemästä päätöksestä voi tehdä valituksen, jolloin kyseistä valvontaviranomaista vastaan nostetaan kanne siinä maassa, jossa hän työskentelee. Rekisteröidyllä on oikeus tehokkaisiin suojakeinoihin, mikäli valvontaviranomainen ei ole informoinut tai käsitellyt asiaa kolmen kuukauden kuluessa valituksesta tai päätöksestä. (EU 2016/679, 80.)

3.5.6 Tietovuodot ja rangaistukset

Vuoden 2012 versiossa tietosuoja-asetuksesta määritellään rekisterinpitäjän velvollisuudet tietovuodon tapahtuessa. Rekisterinpitäjän on ilmoitettava vuodosta viipymättä. Mikäli ilmoitus tehdään yli 24 tuntia tietomurrosta, on rekisterinpitäjän pystyttävä perustelemaan viivästyminen. Rekisterinpitäjän tulee ilmoituksessaan kuvata tietovuoto, arvioida sen mahdolliset seuraukset sekä ilmoittaa vuodon jälkeen tehdyistä toimenpiteistä, joilla haittavaikutuksia on pyritty minimoimaan. Ilmoituksen tulee sisältää tietovuotoa koskevien rekisteröityjen ryhmät ja niiden lukumäärä sekä tietosuojavastaavan tai muun lisätietoa tarjoavan henkilön yhteystiedot. Rekisterinpitäjän täytyy dokumentoida kaikki tietovuotoa koskevat

toimenpiteet, jotta viranomaiset pystyvät tarkistamaan tietosuoja-asetuksen noudattamisen. (COM(2012) 11 final, 62-63.)

Rekisterinpitäjä on velvollinen ilmoittamaan tietovuodosta rekisteröidylle, jos siitä oletetaan koituvan haittaa tämän henkilötietojen suojalle tai yksityisyydelle. Ilmoitus tulee tehdä viipymättä ja siinä tulee tehdä rekisteröidylle selväksi tietovuodon vakavuus, vuodon jälkeiset toimenpiteet sekä ilmoittaa vähintään tietosuojavastaavan yhteystiedot, josta rekisteröity voi halutessaan pyytä lisätietoja. Ilmoitusta ei tarvitse tehdä, jos valvontaviranomainen näkee rekisterinpitäjän tekemät turvatoimenpiteet tietovuodon kohteina olleisiin henkilöihin tarpeeksi vahvoiksi. Valvontaviranomainen voi kuitenkin vaatia rekisterinpitäjää ilmoittamaan asianomaisille tietovuodosta, jos näkee sen tarpeelliseksi. (COM(2012) 11 final, 63-64.)

Henkilötietodirektiiviin ja -lakiin on tehty korjauksia ja nykyisin ne velvoittavat palveluntarjoajia ilmoittamaan tietovuodoista viranomaiselle sekä joissain tapauksissa rekisteröityneelle (Henkilötietolaki 523/1999).

Uusi tietosuoja-asetus tuo mukanaan mahdollisuuden antaa sanktioita tietovuotojen sattuessa. Sanktioita annetaan, mikäli rekisterinpitäjä tai henkilötietojen käsittelijä ei ota huomioon tai jättää tahallaan noudattamatta uuden asetuksen tuomia vaatimuksia. Sanktion maksimimäärä on 20 miljoonaa euroa ja myönnetty sakkomäärä on verrannollinen yrityksen vuotuisiin tuloihin. Jos yritys, jonka globaalista liikevaihdosta 4 % ylittää 20 miljoonaa euroa, määrätään yritykselle maksimimäärä sakkoa. (Andreasson, ym. 2016, 39-40.)

Henkilötietolaki määrittää sakkorangaistuksen henkilörekisteririkkomuksesta. Esimerkiksi tahallisesta tai törkeästä huolimattomuudesta käsittelyn yhteydessä määrätään sakkorangaistus. (Henkilötietolaki 523/1999, 48§.)

Henkilötietodirektiivissä määritellään rekisteröidyn oikeus korvauksiin. Mikäli rekisteröidylle koituu tietovuodosta, lainvastaisesta tietojen käsittelystä tai mistä tahansa asetuksen kanssa ristiriidassa olevasta toiminnasta haittaa, on hän oikeutettu saamaan korvauksia. Korvausvastuuseen henkilötietodirektiivi määrää ainoastaan rekisterinpitäjän. (Henkilötietolaki 523/1999, 47§.)

4 MUUTOKSET

Tässä osiossa käydään läpi tietosuoja-asetuksesta johtuvia käytännön muutoksia. Mitä yritysten tulee ottaa huomioon uudistusten myötä ja kuinka paljon uudet vaatimukset poikkeavat nykyisistä käytännöistä.

4.1 Suomessa

Suomessa ei olla varauduttu uuteen tietosuoja-asetukseen. Tietosuoja perustuu oikeudellisiin normeihin, joiden kautta säädellään yksityisyydensuojaa henkilötietoja käsitellessä. Tietosuojassa on kyse aineellisten oikeuksien ulottamisesta informaatiota koskeviksi. Organisaatiot joutuvat miettimään ja muokkaamaan toimintamallinsa uudestaa, jotta tietosuoja-asetusta ei rikottaisi. Suomessa koko tietosuojan erityislainsäädäntö joudutaan arvioimaan uudestaa, sillä kansallinen lainsäädäntö ei voi olla ristiriidassa uuden tietosuoja-asetuksen kanssa. (Andreasson, ym. 2014, 18.)

Asetus koskee kuitenkin hyvin laajaa kohderyhmää, sillä se vaikuttaa niin pieniin kuin suuriin yrityksiin, myös julkisiin ja yksityisiin. Ennen uutta asetusta ainoastaan sosiaali- ja terveyshuollolta sekä pankeilta ja vakuutusyhtiöiltä on vaadittu korkean tason tietosuojaa. Sosiaali- ja terveysalalla tietosuojavastaavan nimittäminen tuli lakisääteiseksi vuonna 2007. Vielä muutama vuosi sitten yritykset jakoivat tietosuojan eri osiin. Uusi asetus pakottaa kuitenkin yritykset muuttamaan ajatusmallejaan ja näkemään tietosuojan isona kokonaisuutena. (Andreasson, ym. 2014, 18.)

Uuden asetuksen mukana astuu voimaan myös pakote, jonka mukaa julkisen sektorin organisaatioiden on nimettävä tietosuojavastaava. Vastaavasti yksityisellä sektorilla yritykset, jotka seuraavat toiminnassaan paljon henkilötietoja, kuten verkkokaupat, joutuvat nimittämään tietosuojavastaavan. Suuri osa suomalaisista yrityksistä on kuitenkin nimittänyt tietosuojavastaavan jo ennakkoon varmistakseen työntekijöidensä tietosuojaosaamisen. (Andreasson, ym. 2016, 36.)

4.2 Euroopassa

EU:n uusi asetus tuo mukanaan paljon uudistuksia totuttuihin käytäntöihin. Käsitteiden määrittelemisestä tulee tärkeämpää. Ennen oli hyväksyttävää jos yritys päällisin puolin näytti toimivan asetusten puitteissa. Yritysten ei esimerkiksi tarvinnut todistaa noudattavansa vanhaa asetusta. Uuden tietosuoja-asetuksen myötä yritysten täytyy kyetä todistamaan noudattavansa tietosuojalainsäädäntöä. Velvollisuus ilmoittaa suurista tietoturvaloukkauksista on myös iso muutos. Rekisterinpitäjälle asetetaan paljon uusia vaateita. Täytyy pystyä tukemaan tietosuojavastaavaa töissään, tarjota rekisteröityneelle mahdollisuus saada henkilötietonsa koneluettavassa muodossa nopeasti pyynnöstä tai antaa mahdollisuus siirtää tietonsa toiselle rekisterinpitäjälle. Uudet asetukset säädetään tietosuojaviranomaisen tehtävien, toimintakentan ja valtuuksien pohjalta. (Andreasson, ym. 2016, 39-40.)

Tietosuojaviranomainen on toimivaltainen ainoastaan oman maansa sisällä. Rajojen ylittyessä toimivaltainen viranomainen on se, jossa rekisterinpitäjän päätoimipaikka sijaitsee. Jos rekisterinpitäjän toimipaikka on Suomessa, suomen viranomaiset käsittelevät asian. Yhteistyön tärkeyttä ei myöskään ole unohdettu. Tästä syystä perustettiin Euroopan tietosuojaneuvosto, jonka tavoitteena on tukea tietosuojaviranomaisten kansainvälistä yhteistyötä. Tietosuojaneuvostolle luodaan oikeus antaa sitovia päätöksiä asetusten soveltamiseksi. Isona muutoksena tulee myös valvontaviranomaisen oikeus määrätä hallinnollisia seuraamuksia. Rikkomuksista rangaistessa voi valvontaviranomainen määrätä jopa 20 miljoonan euron suuruisen sakon. Jos organisaation globaalista liikevaihdosta 4 % on yli 20 miljoonaa euroa, tulee sakolle maksimimäärä. (Andreasson, ym. 2016, 40.)

Asetuksen mukana tuodaan erityisesti esille rekisteröidyn oikeudet. Samalla pyritään vahvistamaan henkilön mahdollisuuksia kontrolloida omien henkilötietojensa käsittelyä. Henkilölle on tehtävä selväksi, että hän on suostumassa henkilötietojen keräämiseen. Henkilöllä on myös oikeus peruuttaa suostumuksensa tietojen keräämiseen, milloin vain hän haluaa. Kaikilla on oikeus tulla unohdetuksi, jos he niin haluavat. Rekisterinpitäjän velvollisuudet muuttuvat vanhoista siten, että rekisterinpitäjän on annettava rekisteröidylle enemmän tietoja henkilötietojen käsittelystä, ja tuoda esiin prosessin läpinäkyvyyttä. Rekisteröidyn

oikeudet eivät juurikaan muutu henkilötietolaissa jo määritellyistä oikeuksista. Rekisteröidyllä on edelleen oikeus oikaista valheellisia tietoja ja tietää minkälaisia tietoja hänestä on kerätty. Asetuksen myötä uutena tulee rekisteröidyn oikeus saada hänestä kerätyt tiedot sähköisessä muodossa, sekä mahdollisuus siirtää tiedot toiseen järjestelmään entistä vaivattomammin. Rekisteröidyllä on myös oikeus tehdä valitus valvontaviranomaiselle. Rekisteröity voi käyttää oikeussojakeinoja sekä saada korvauksia. Henkilöllä on oikeus tarkastuttaa viranomaisten tekemä päätös kansallisessa tuomioistuimessa, vaikka rekisterinpitäjä olisi eri valtiosta. (EU 2016/679.)

Uusi asetus tiukentaa myös sen noudattamista. Asetuksessa luetellaan erikseen henkilötietojen käsittelijää koskevat velvollisuudet. Käsittelijän velvollisuutena on esimerkiksi toteuttaa toimenpiteitä tietosuojaan liittyen. Toimenpiteiden vaadittava laajuus on riippuvainen olemassa olevan riskin suuruudesta tietojenkäsittelyn yhteydessä. Tietosuojavastaavan nimittämisestä tulee pakollista julkiselle sektorille ja osalle yksityistä sektoria. Mikäli yksityisyritys toteuttaa riskialttiita toimia tietojenkäsittelyssään, tulee yrityksen nimetä tietosuojavastaava. (Andreasson, ym. 2016, 12.)

Euroopan unionin jäsenvaltiot ovat velvollisia nimeämään valvontaviranomaisen. Tietosuojalainsäädännöt ovat ennen uutta asetusta olleet valtioiden omissa käsissä mutta uusi asetus pyrkii luomaan yhtenäisen johdonmukaisemman lainsäädännön. Johdonmukaisuutta pyritään edistämään esimerkiksi sillä, että rajat ylittävissä tapauksissa tehdään vain yksi päätös. Yrityksiä tämä helpottaa siten, etteivät he joudu olemaan yhteydessä useampaan kuin yhden valtion valvontaviranomaiseen. Tietosuoja-asetuksen mukana perustetaan myös Euroopan tietosuojaneuvosto, joka koostuu valvontaviranomaisten 28:sta edustajasta. Neuvosto korvaa nykyisen komitean. (EU 2016/679.)

Mainittakoon tiedonsiirrosta kolmansiin maihin sen verran, että jos maalla ei ole komission mielestä riittävää tasoa tietosuojassa, ei tietoja saa siirtää kuin erityistapauksissa (EU 2016/679).

5 YHTEENVETO

Euroopan unionin käsitys tietosuojasta ei ole ennen uutta asetusta ollut ajantasainen. Päivityksistä huolimatta asetukset tietoturvaan ja tietosuojaan pohjautuvat pitkälti ennen 2000-lukua voimaan astuneisiin henkilötietodirektiiviin sekä henkilötietolakiin. Jäsenmaat ovat toimineet omien lakiensa puitteissa, eikä unionin sisällä ole ollut yhteistä linjaa. Kun vielä käytössä olevat asetukset pohjautuvat aikaan, jolloin noin 1–2 % eurooppalaisista omistivat internetyhteyden, on muutos tervetullut.

Tietoa verkossa kulkee päivä päivältä enemmän ja uudeksi huolenaiheeksi on kasvanut henkilötietojen käsittely. Internetissä kulkee tietoa ihmisen olinpaikasta, tekemisistä ja käydyistä keskusteluista ja niitä kerätään pahimmissa tapauksissa kertomatta. Jokaisella on oikeus omaan yksityiselämään ja tietoon siitä kuka henkilökohtaisia tietoja käsittelee. Uusi tietosuoja-asetus pyrkii luomaan tietojenkäsittelyn prosessista läpinäkyvämpää ja tuomaan käyttäjälle päätösvaltaa henkilötietojensa suhteen.

Opinnäytetyössä pyrittiin keräämään tietoa tietosuoja-asetuksen taustoista ja sen muutoksista aiempaan lainsäädäntöön nähden. Muutoksia pyrittiin tarkastelemaan yrityksen, rekisterinpitäjän ja rekisteröidyn kannalta, jotta asiasta saataaisiin mahdollisimman kattava kuva.

Uuden asetuksen johdosta rekisteröidyn valta tietojenkäsittelyssä kasvaa. Rekisteröity henkilö saa vallan päättää, antaako henkilötietonsa käsiteltäväksi ja voi halutessaan muuttaa mielipidettään. Rekisteröidyllä on oikeus nähdä, poistattaa tai siirtää tiedot, joita häneltä on kerätty, sekä oikeus tulla unohdetuksi, jos siihen tarvittavat vaatimukset nähdään täyttyvän.

Rekisterinpitäjän osalta uusi tietosuoja-asetus kasvattaa vastuuta. Asetus pyrkii tekemään tietojen suojaamisesta oletusarvoista jo olemassa olevissa palveluissa ja ohjelmistoissa, sekä uusien suunnittelussa ja toteutuksessa. Uutena velvollisuutena rekisterinpitäjälle tulee vaikutustenarviointi, jonka tarvittavuus määritellään tapauskohtaisesti. Rekisterinpitäjän täytyy pystyä todistamaan seuraavansa tietosuoja-asetuksen säädöksiä. Hän on myös velvollinen pitämään

kirjaa jokaisesta henkilötietojen käsittelystä. Asetus myös velvoittaa rekisterinpitäjää suojaamaan henkilötietoja asianmukaisella tekniikalla ja metodeilla. Ennen asetusta rekisterinpitäjä oli yksin vastuussa tietosuojasta ja tietoturvasta, mutta nyt vastuu ulottuu myös tietojen käsittelijään.

Ennen uutta asetusta tietosuojavastaavan tehtävät eivät olleet pakollisia muilla aloilla kuin sosiaali- ja terveysalalla. Tietosuojavastaavan tehtäviin kuuluu organisaation tietosuoja-asioista huolehtiminen, rekisterinpitäjän apuna toimiminen sekä organisaation tietosuoja-asioiden suunnittelemisen ja toteutuksen seuraaminen ja niissä avustaminen. Tietosuojavastaava ei ole vastuussa tietoturvasta. Tietosuojavastaavan nimittäminen on pakollista, jos henkilötietojen käsittelyä ei ole suorittamassa viranomainen, julkishallinto tai tuomioistuin. Nimittäminen on pakollista myös tilanteissa, joissa organisaation ydintoimintaan kuuluu henkilötietojen käsittelyä, joka vaatii laajamittaista seurantaa.

Suomessa uuteen asetukseen valmistautuminen vaatii paljon työtä. Etenkin aineellista omaisuutta koskevien lakien laajentaminen informaatiota koskeviksi on iso askel. Asetus pakottaa organisaatioita muuttamaan käsityksiään tietoturvasta ja näkemään sen osana isompaa kokonaisuutta. Asetusten seuraamisesta tulee entistä tarkempaa, sillä rikkomuksista johtuvien sanktioiden määrä kasvaa. Jos organisaation globaalista liikevaihdosta 4 % on yli 20 miljoonaa euroa, tulee sakosta maksimikokoinen eli 20 miljoonaa euroa.

Opinnäytetyön tavoitteet saavutettiin. Uuden tietosuoja-asetuksen taustoista löydettiin tietoa. Myös muutoksista löydettiin tietoa ja niitä verrattiin edeltäviin asetuksiin henkilötietolakiin ja henkilötietodirektiiviin, joista aiemmat määritelmät ovat peräisin. Lisäksi käytiin läpi ongelmakohtia, joita uuden asetuksen luomisen varrella tuli vastaan.

6 POHDINTA

Uusi asetus tulee ja se on lähtökohtaisesti hyvä asia. Euroopassa lait eivät ole pysyneet mukana teknologian kehityksen ja internetin hyödyntämisen kanssa. Yhtenäistä näkökulmaa tiedon siirtämiseen ja käsittelemiseen maiden välillä ei ole ollut, ja jokainen maa on kyseisen asian tiimoilta toiminut omien asetustensa puitteissa. Jäsenmaiden yhtenäisen asetuksen rakentaminen olisi pitänyt aloittaa jo vuosia aiemmin, jotta näin suuri muutos olisi voitu välttää.

Uudistukset tuovat varmasti mukanaan ongelmia. Tietosuoja-asetus on vain kuvainnollinen luuranko, jonka ympärille tullaan tarkentavilla asetuksilla rakentamaan lihaa. Muutokset eivät voi koskaan olla alusta lähtien täydellisiä, sillä jokaista mahdollisuutta tulkita asetusta on mahdotonta ennustaa.

Opinnäytetyössä mainittu esimerkki Googlen ja Ranskan kiistasta antaa ajattelemisen aihetta (Tivi, 2016). Onko jo liian myöhäistä tehdä asetuksia, jotka koskevat vain tiettyä ryhmää, kuten Euroopan unionia? Internet ei sinänsä käsitä maiden rajoja. Tulli ei tule kyselemään passia, jos vierailee amerikkalaisella sivustolla. Internettiä ja sielä liikkuvaa dataa tulisi ajatella globaalilta näkökannalta. Esimerkiksi Euroopassa asetettujen lakien tulisi pysyä Euroopan rajojen sisäpuolella, eikä ulkopuolisen valtion tulisi joutua tilanteeseen, jossa maan sisällä tapahtuvissa asioissa tulisi ottaa huomioon ulkopuolisia lainsäädäntöjä. Se on absurdia.

Sen sijaan että globaalisti toimivaa internetverkkoa aletaan säätelemään pahimmillaan maakohtaisesti, olisi kaikkien kannalta parempi vaihtoehto luoda yhteinen tiedonkäsittelylaki, jota voitaisiin hyödyntää jokaisessa valtiossa ja unionissa samalla tavalla. Idea on kuitenkin täysin idealistinen ja kaatuisi omaan mahdottomuuteensa. Eri maiden kulttuurierot ja muut näkökannalliset eroavuudet johtaisivat siihen, että yhteistä näkökulmaa asiaan ei tultaisi koskaan löytämään.

Toinen vastaan tullut ongelmakohta on Iso-Britannia. Uuttaa asetusta aloitettiin rakentamaan jo kauan ennen Iso-Britannian eroamista Euroopan Unionista. Tästä huolimatta Iso-Britannian on velvollinen noudattamaan EU:n asettamaa tietosuoja-asetusta niissä tapauksissa, joissa Iso-Britanniassa toimiva organisaatio käsittelee

Euroopan uuden tietosuoja-asetuksen turvaamia henkilötietoja eli eurooppalaisten henkilötietoja. Tämä on paras mahdollinen kompromissi, mutta ei silti poista ajatusta siitä, että pian Euroopan unionista täysin erillään olevaa valtiota velvoitetaan noudattamaan heille ulkopuolisia asetuksia. (IT Governance [Viitattu 26.3.2017].)

Huomiota myös herätti rekisterinpitäjien vastuumäärän kasvaminen. Rekisterinpitäjillä on varmasti ollut jo ennen asetuksien voimaan astumista kädet täynnä töitä. Tuntuu oudolta, että suurin osa muutoksista aiheutuvista velvollisuuksista asetetaan yhden ammattiryhmän päälle. Toki joitain osia vastuusta on jaettu useammalle taholle, mutta asiaa tutkiessa tuntui, että rekisterinpitäjä on ainakin jollain tasolla velvollinen lähes joka asiaan.

Yristysten kannalta muutokset ovat pääasiassa hyviä. Varsinkin niille organisaatioille, jotka ovat paljon tekemisissä tiedonsiirron kanssa muihin maihin. Näkökannan suoraviivaistaminen on heille varmasti positiivista. Isot muutokset, kuten asetuksen omaksuminen, siihen valmistautuminen sekä tietosuojan ja tietoturvan muuttaminen ajattelutavassa lähtökohtaiseksi, vaativat kuitenkin aikaa ja resursseja.

Yksityishenkilöjen kannalta muutokset ovat myös positiivista. Lisääntyvä kontrolli siihen, miten henkilötietoja käsitellään on hyvä asia. Mutta muuttaako tämä käytännössä kuitenkaan mitään? Voidaan todeta faktana se, että hyvin pieni osa lukee internetiä selatessaa ja sivustoille rekisteröityessään käyttöehdot. Tulevaisuudessa rekisteröidyn oikeudet upotetaan sivustoille todennäköisesti samalla tavoin kuin käyttöehdot. Tapaus, jossa käyttäjää pyydetään rastittamaan jokin kohta merkkinä henkilötietojen keräämisen ja käsittelyn hyväksymiseen tulee olemaan tuttu ilmiö kaikille. Valitettavasti nämä tullaan ohittamaan, ja hyvin harva rekisteröitynyt tulee koskaan tietämään uusista oikeuksistaan. Onko osasyynä uuden tietosuoja-asetuksen taustalla ollut saada hiljaiseksi se pieni, mutta äänekäs osa väestöstä, jolle verkossa tapahtuva tietojen kerääminen on ollut viime vuosina ylitsepääsemätön paha?

LÄHTEET

Aarnio, R. 2015. Mitä tietosuoja tarkoittaa? [www-sivu]. Tietosuojavaltuutetun toimisto. [Viitattu 22.2.2017]. Saatavilla: https://koulutus.fcg.fi/Portals/2/Dokumentit/Reijo%20Aarnio%20MIT%C3%84%20TIETOSUOJA%20TARKOITTAA%5BCompatibility%20Mode%5D.pdf

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma Oy.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma Oy.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma Oy.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. 2. uudistettu laitos. 3. painos. Helsinki: Tietosanoma Oy.

COM(2012) 9 final. 2012. Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealla ja alueiden komitealle. [www-sivu]. Euroopan komissio. [Viitattu 11.2.2017]. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012DC0009&from=EN

COM(2012) 10 final. 2012. Euroopan parlamentin ja neuvoston direktiivi. [www-sivu]. Euroopan komissio. [Viitattu 11.2.2017]. Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:fi:PDF

COM(2012) 11 final. 2012. Euroopan parlamentin ja neuvoston asetus. [www-sivu]. Euroopan komissio. [Viitattu 11.2.2017]. Saatavilla: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fi.pdf

Eurooppa-neuvosto. 2010. Tukholma-ohjelma 2010/C 115/01. [www-sivu]. Euroopan unioni. [Viitattu 2.3.2017]. Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:fi:PDF

EU 2000/C 364/01. 2000. Euroopan unionin perusoikeuskirja. [www-sivu]. Euroopan unioni. [Viitattu 4.1.2017]. Saatavilla: http://www.europarl.europa.eu/charter/pdf/text_fi.pdf

EU 2016/679. 2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. [www-sivu]. Euroopan unioni. [Viitattu 17.1.2017]. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

EU 95/46/EY. 1995. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY. [www-sivu]. Euroopan unioni. [Viitattu 3.1.2017]. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:31995L0046&from=fi

Henkilötietolaki 523/1999. 1999. Henkilötietolaki. [www-sivu]. Oikeusministeriö. [Viitattu 9.3.2017]. Saatavilla: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Internet world stats. 2015. Internet penetration in Europe November 2015. [www-sivu]. Miniwatts Marketing Group. [Viitattu 20.2.2017]. Saatavilla: http://www.internetworldstats.com/stats4.htm

IT Governance. Ei päiväystä. The EU General Data Protection Regulation (GDPR). [www-sivu]. IT Governance Ltd. [Viitattu 26.3.2017]. Saatavilla: https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

Lehtonen, K. 2014. Mitä jokaisen tulisi tietää tietosuojasta ja tietoturvasta juuri nyt? [www-sivu]. TRUST Asianajotoimisto Oy. [Viitattu 1.2.2017]. Saatavilla: https://www.slideshare.net/Janklindberg/ict-expo-08052014-kiira-lehtonen

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. Helsinki: Kauppakamari Oy.

Niemi. M-L. 2016. Oikeus tänään. 4. uudistettu painos. Rovaniemi: Lapin yliopisto.

Oikeusministeriö. 2015. Kysymyksiä ja vastauksia tietosuojauudistuksesta. [www-sivu]. Oikeusministeriö. [Viitattu 7.2.2017]. Saatavilla: http://oikeusministerio.fi/material/attachments/om/valmisteilla/lakihankkeet/informaatio-oikeus/xB1Vydn8T/Kysymyksia_ja_vastauksia_tietosuojasta.pdf

OM2015-00233. 2015. Yleinen tietosuoja-asetus. [www-sivu]. Oikeusministeriö. [Viitattu 11.3.2017]. Saatavilla: https://www.eduskunta.fi/FI/vaski/Liiteasiakirja/Documents/U_21+2012.pdf

Rovamo, O. 2016. Tietosuoja ja standardit. [www-sivu]. Suomen Standardoimisliitto SFS ry. [Viitattu 18.3.2017]. Saatavilla: https://www.slideshare.net/SuomenStandardisoimisliitto/eun-yleinen-tietosuojaasetus-keskeisimmt-uudet-asiat

Tivi. 2016. ”Kohta kaikki maat vaativat samaa” – Google riitelee Ranskan kanssa saamistaan 100 000 euron sakoista. [www-sivu]. Talentum. [Viitattu 23.2.2017]. Saatavilla: http://www.tivi.fi/Kaikki_uutiset/kohta-kaikki-muut-maat-vaativat-samaa-google-riitelee-ranskan-kanssa-saamistaan-100-000-euron-sakoista-6552367

U 21/2012 vp. 2015. Komission ehdotus asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus). [www-sivu]. Valtioneuvosto [Viitattu 20.4.2017].

Saatavilla: https://www.eduskunta.fi/FI/vaski/Liiteasiakirja/Documents/U_21+2012.pdf

Ulkoasiainministeriö. 2015. Schengen-maiden yhteinen viisumitietojärjestelmä laajenee kaikkiin maihin. [www-sivu]. Ulkoasiainministeriö. [Viitattu 13.1.2017]. Saatavilla: http://formin.finland.fi/public/default.aspx?contentid=333627&contentlan=1&culture=fi-FI

Vahti. 2016. EU-tietosuojan kokonaisuudistus. Vahti-raportti 1/2016. [www-sivu]. Valtiovarainministeriö. [Viitattu 26.1.2017]. Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Vanto. J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro Oy.