

Taru Väisänen

**EU:N YLEINEN TIETOSUOJA-ASETUS JA SEN VAIKUTUKSET OULUN
AMMATTIKORKEAKOULU OY:SSÄ**

EU:N YLEINEN TIETOSUOJA-ASETUS JA SEN VAIKUTUKSET OULUN AMMATTIKORKEAKOULU OY:SSÄ

Taru Väisänen
Opinnäytetyö
Kevät 2015
Liiketalouden koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Liiketalouden koulutusohjelma, oikeuden ja hallinnon suuntautumisvaihtoehto

Tekijä: Taru Väisänen

Opinnäytetyön nimi: EU:n yleinen tietosuoja-asetus ja sen vaikutukset Oulun ammattikorkeakoulu Oy:ssä

Työn ohjaaja: Ulla Tarvainen

Työn valmistumislukukausi- ja vuosi: Syksy 2015

Sivumäärä: 45 + 1

Tämän opinnäytetyön aiheena on Euroopan unionin yleinen tietosuoja-asetus, jonka arvellaan tulevan voimaan vuoden 2015 loppuun mennessä. Valmisteltavana olevan asetuksen tavoitteena on lainsäädännön ja oikeuskäytännön yhtenäistäminen unionin alueella. Nykyinen direktiivimuotoinen säädös on aiheuttanut tietosuojan eritasaisuuden jäsenmaiden kesken. Asetus tuo rekisterinpitäjille uusia velvoitteita ja parantaa rekisteröidyn asemaa ja hänen oikeuksiaan.

Työn tavoitteena on selvittää, miten henkilötietojen säätely muuttuu asetuksen myötä, ja miten nämä muutokset vaikuttavat rekisterinpitäjän, tämän työn tapauksessa toimeksiantajana olevan Oulun ammattikorkeakoulu Oy:n toimintaan. Opinnäytetyön tutkimusmenetelmä on lainoppi, pääasiallisina lähteinä ovat oikeushierarkian mukaisesti laki ja lainvalmisteluasiakirjat. Työssä vertaillaan tulevaa yleistä tietosuoja-asetusta ja sen säädöksiä tämän hetkisiin säädöksiin; Euroopan unionin Henkilötietodirektiiviin 95/46/EY sekä Suomen henkilötietolakiin 22.4.1999/523. Koska asetuksen sisältö muokkautuu parlamentin ja neuvoston yhä sitä käsitellessä, työssä käytetään tietosuoja-asetusehdotusta COM(2012)11 final, jonka sisältö voi poiketa lopullisesta säädettävästä asetuksesta. Työssä käytetään lisäksi laadullisen tutkimuksen keinoja haastattelemalla kolmea Oulun ammattikorkeakoulun työntekijää. Näiden haastattelujen tarkoituksena on selvittää tietosuojan nykyhetkinen taso ja varautuminen tulevaan lainsäädäntöön.

Työn tuloksina selvisi, että tietosuojan taso Oulun ammattikorkeakoulussa on tällä hetkellä hyvä, eikä uuden tietosuoja-asetuksen tuleminen aiheuta suuria toimenpiteitä. Rekistereiden ajantasaisuuteen ja henkilöstön tietosuojaosaamiseen on kuitenkin kiinnitettävä huomiota. Tietosuojavastaavan määräämisen koetaan selkeyttävän vastuunjakoja tietosuoja-asioissa sekä lisäävän selkeyttä henkilörekisterijärjestelmään. Jatkotutkimusaiheena voisi selvittää, miten hyvin tietosuoja-asetuksen toteuttamisessa on onnistuttu Oulun Ammattikorkeakoulussa.

Asiasanat: EU-oikeus, henkilötieto, tietosuoja, yksityisyys

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Economics, Option of Law and Administration

Author: Taru Väisänen

Title of thesis: EU data protection regulation and its effects in Oulu University of Applied Sciences

Supervisor: Ulla Tarvainen

Term and year when the thesis was submitted: Autumn 2015 Number of pages: 45 + 1

The topic of this thesis deals with EU data protection regulation, which is supposed to come into force before the end of the year 2015. The purpose of this regulation currently under preparation is to standardize the legislation and legal praxis within the European Union. Current degree which is the directive has led the data protection to differ between member countries. The regulation brings new obligations to registration authority and improves the status and rights of a registered person.

The aim of this thesis is to examine how the regulation of personal data alters along with the regulation and how these changes affect Oulu University of Applied Sciences which is commissioner of this thesis. The thesis method is jurisprudence and primary sources consist of law and law drafting documents. The thesis compares EU data protection regulation to effective statutes; EU Data Protection Directive 95/46/EC and Finnish Personal Data Act 22.4.1999/523. Since the new regulation will still furthermore be modified, the content might differ from the final regulation. This thesis also employs qualitative research including interviews with three employees of Oulu University of Applied Sciences. The purpose of these interviews is to establish the present level of data protection and to prepare for prospective changes in legislation.

The results of thesis indicate that the level of data protection is good at the moment, and the regulation will not call for any major legislative action. Keeping the person register up-to-date and improving personnel's skills on data security has to be paid attention to. Appointing of a data protection officer is considered to clarify liabilities in data protection and to simplify person register system. A topic for further study could deal with a follow-up on how successfully the regulation has been implemented in Oulu University of Applied Sciences.

Keywords: data security, EU legislation, personal data, privacy

LYHENTEET

HE	Hallituksen esitys
Henkilötietodirektiivi	Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
HeTil	Henkilötietolaki 22.4.1999/523
OECD	Organisation for Economic Cooperation and Development
OAMK	Oulun ammattikorkeakoulu Oy
OSA	Oikeus- ja sisäasioiden neuvosto
SVT	Suomen virallinen tilasto
Tietosuoja-asetus	Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta COM(2012)11 final

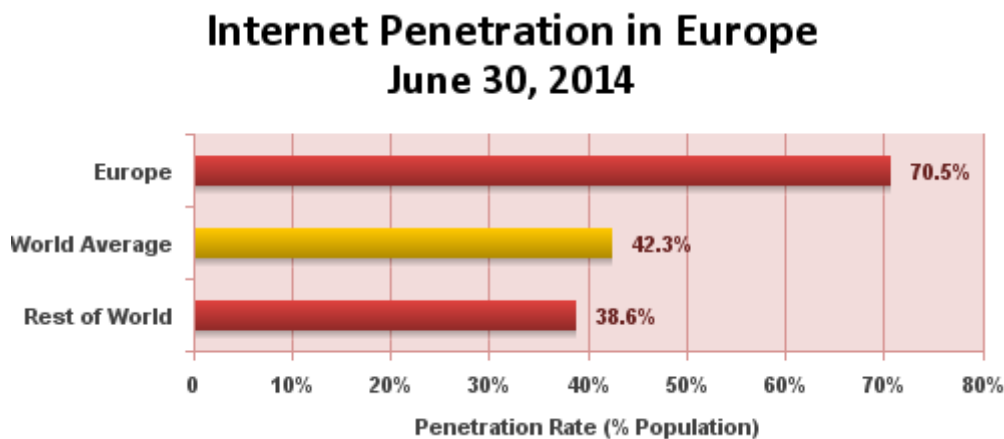
SISÄLLYS

LYHENTEET.....	5
1 JOHDANTO.....	7
2 TIETOSUOJA.....	12
2.1 Tietosuojalainsäädännön kehitys	12
2.2 Yleiset käsitteet	14
3 OAMK.....	19
3.1 Organisaatio	19
3.2 Tietosuoja Oamkissa.....	20
4 TIETOSUOJA-ASETUS.....	21
4.1 Taustaa	21
4.2 Rekisterinpitäjän velvollisuudet	23
4.2.1 Yleiset velvollisuudet.....	23
4.2.2 Sisäänrakennettu ja oletusarvoinen tietosuoja sekä tietoturvallisuus.....	24
4.2.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkohyväksyntä	24
4.2.4 Tietosuojavastaava	26
4.2.5 Tietovuodot ja sanktiot	26
4.3 Rekisteröidyn oikeudet	29
4.3.1 Läpinäkyvyys ja tiedonsaantioikeus	29
4.3.2 Tietojen oikaiseminen, poistaminen ja oikeus tulla unohdetuksi	30
4.3.3 Oikeus vastustaa henkilötietojen käsittelyä ja profilointia	31
4.3.4 Oikeussuojakeinot.....	32
5 VAIKUTUKSET OULUN AMMATTIKORKEAKOULUSSA.....	34
5.1 Tietosuoja ja sen uudistuminen Oamkissa	34
5.2 Tietosuojavastaava	35
5.3 Rekisteröidyn asema.....	36
6 JOHTOPÄÄTÖKSET	38
7 POHDINTA.....	40
LÄHTEET.....	42
LIITTEET	

1 JOHDANTO

Henkilötietojen jakaminen on arkipäiväistänyt Internetin ollessa yhä suurempi osa jokapäiväistä elämää; verkkokaupoista tilaaminen tai sosiaalisessa mediassa oleminen on yhä yleisempää. Henkilötietoja saatetaan luovuttaa esimerkiksi rekisteröintitilanteessa enemmän kuin on tarpeen, ja tietosuojaselosteiden lukeminen ohitetaan rastittamalla ”Hyväksyn palvelun ehdot” -ruutu asiaa tarkemmin miettimättä. Samalla kuitenkin tietovuodoista uutisoidaan julkisuudessa aiempaa enemmän, ja ne kohdistuvat aina valtion organisaatioista pieniin yrityksiin. Pankkikorttitietoja voidaan kaapata, puhelinnumeroa, osoitetta tai nettiin lähipiirille jaettuja, yksityisiksi tarkoitettuja kuvia ja tarinoita saatetaan levittää julkisesti.

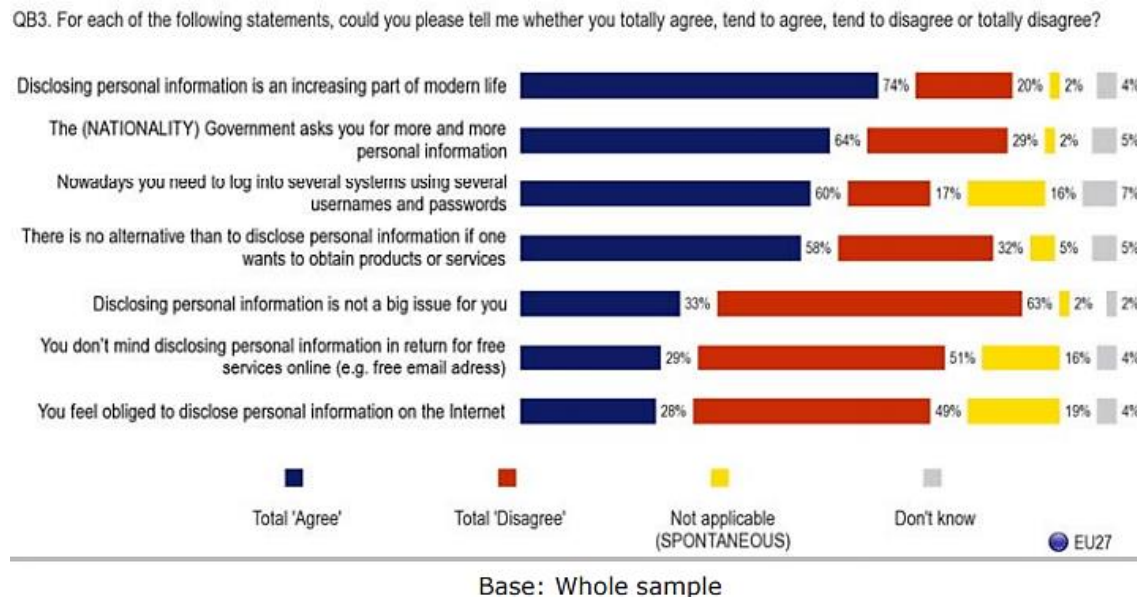
Eurooppalaiset ovat pohjoisamerikkalaisten ohella ahkerimpia Internetin käyttäjiä. Keski- ja Pohjois-Euroopan maissa Internetiä käyttää lähes koko väestö, esimerkiksi Luxemburgissa Internetiä käyttää 98 % väestöstä, Belgiassa 90,4 % ja Saksassa 88,6 %. Itä-Euroopassa esimerkiksi Ukrainassa, Moldovassa ja Valko-Venäjällä vain noin puolet kansasta käyttää Internetiä. (Internet World Stats, viitattu 29.4.2015.) Teknologian kehittyessä ja halventuessa näiltä alueilta on odotettavissa miljoonia uusia Internet-käyttäjiä.



KUVIO 1. Internet Penetration in Europe June 30, 2014 (Internet World Stats, viitattu 29.4.2015)

Euroopan komission 16.6.2012 julkaisemassa eurobarometrissa (Eurobarometri nro 359) tutkittiin kansalaisten asenteita tietosuojaa ja yksityisyyttä kohtaan. Kyselyssä selvitettiin muun muassa sitä, kuinka laajaksi ihmiset mieltävät henkilötietokäsittelyn, kuinka hyvin he kokevat pystyvänsä itse määräämään omista tiedoistaan ja kuinka he suhtautuvat tietojensa luovuttamiseen.

Barometrissa vuonna 2011 haastatelluista 26 574 eurooppalaisesta 66 % käyttää Internetiä, 39 % tekee ostoksia verkossa, 34 % käyttää sosiaalisen median sivuja ja 29 % jakaa kuviaan, videoita ja elokuvia erilaisilla nettisivuilla (European Commission 2015b, 39, viitattu 29.4.2015). Eurobarometrin tuloksista selviää, että henkilötietojen luovuttaminen koetaan osaksi nykyelämää, joissain tilanteissa jopa välttämättömäksi tai kuten 28 % vastaajista koki, pakolliseksi toimenpiteeksi Internetissä (European Commission 2015b, 22, viitattu 29.4.2015).

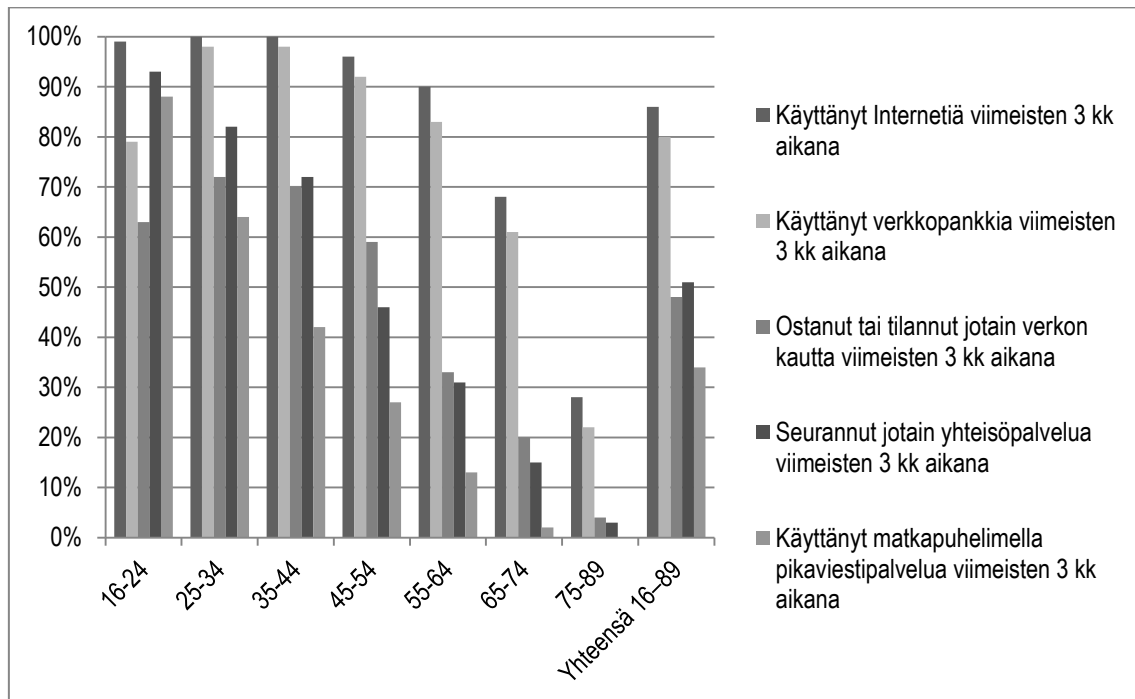


KUVIO 2. Perception of the necessity of disclosing personal information. (European Commission 2015b, 22, viitattu 29.4.2015.)

Barometriin vastanneista 62 % antaa minimimäärän informaatiota suojellakseen identiteettiään. Yleisimmin sosiaalisessa mediassa annettavat tiedot ovat nimi (79 %) ja valokuvat (51 %), Internetissä ostoksia tekeillä taas nimi (90 %) ja kotiosoite (89 %). (European Commission 2015b, 40, 100.) Internetin välityksellä ostoksia tehneistä vain 18 % kokee täyden vallan muuttaa, poistaa tai korjata antamiaan tietoja (European Commission 2015b, 129, viitattu 29.4.2015). Kaikista vastaajista 70 % on huolissaan siitä, että yritykset käyttävät hallussaan olevia henkilötietoja muuhun kuin keräämisvaiheessa ilmoitettuun tarkoitukseen (European Commission 2015b, 2, viitattu 29.4.2015). Eurobarometrin tuloksista selviää, että eurooppalaiset ovat yhä huolestuneempia yksityisyydestään.

Suomessa Internetin käyttö on eurooppalaista keskitasoa yleisempää. Tilastokeskuksen 6.11.2014 julkaiseman *Väestön tieto- ja viestintätekniikan käyttö -tutkimus 2014:n* mukaan 86 % 16–89 -vuotiaista suomalaisista käyttää Internetiä. 16–44 -vuotiaista lähes kaikki käyttävät

Internetiä, vanhemmilla ikäryhmillä käyttöaste on matalampi. Viimeisen kolmen kuukauden aikana 48 % oli tehnyt ostoksia Internetin välityksellä.



KUVIO 3. Internetin käytön ja eräiden Internetin käyttötapojen yleisyys 2014 (SVT 2014, viitattu 28.4.2015)

Henkilötietojen suojasta säädetään tällä hetkellä direktiivimuotoisella EU-säädöksellä, joka on aiheuttanut tietosuojan tason vaihtelevuuden EU-valtioiden välillä. Esimerkiksi ilmoitusvelvollisuus tietosuojaviranomaiselle vaihtelee jäsenvaltioiden kesken, mikä tuo ongelmia kansainvälisille yrityksille (Pitkänen, Tiilikka & Warma 2013, 26). Eurobarometristakin ilmennyt epäluottamus sähköisiin toimijoihin halutaan lainsäätäjän toimesta muuttaa niin, että sähköisille markkinoille luodaan yhteiset pelisäännöt – koskien myös ei-eurooppalaisia, EU-kansalaisille palveluita tarjoavia yrityksiä. (European Commission 2015c, viitattu 22.4.2015.)

Euroopan komissio ryhtyi uudistamaan unionin tietosuojalainsäädäntöä tiedonannolla 2010, ja noin kahden vuoden valmistelun jälkeen antoi 29.1.2012 ehdotuksen COM(2012) 11 final Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus). Tietosuoja-asetuksen tavoitteena on ajanmukainen ja yhtenäinen tietosuojakehys sekä digitaalisten sisämarkkinoiden kehittäminen Euroopan unionin alueella. (Oikeusministeriö 2014, viitattu 15.12.2014.)

Yleisen tietosuoja-asetuksen on tarkoitus tulla voimaan vuoden 2015 lopussa tai vuoden 2016 alkupuolella. Asetusehdotus on käsitelty ja hyväksytty parlamentissa jo maaliskuussa 2014, mutta neuvosto pääsi yksimielisyyteen asetuksen sisällöstä vasta kesäkuussa 2015. Asetusta on kritisoitu muun muassa sen säätämisen hitaudesta. Vaikka asetus pyritään säätämään teknologiariippumattomaksi, suurimmat kritikat epäilevät sen olevan vanhentunut jo voimaan tullessaan.

Tämän opinnäytetyön tarkoituksena on selvittää

- Millaisia muutoksia EU:n uusi yleinen tietosuoja-asetus tuo lainsäädäntöön?
- Miten Oamk Oy:n tulee varautua toiminnassaan tietosuoja-asetuksen velvoitteisiin?
- Miten tietosuoja-asetus vaikuttaa rekisteröidyn asemaan Oamk Oy:ssä?

Opinnäytetyö on lainopillinen tutkimus, jonka tietoperustana on oikeushierarkian mukaisesti kirjoitettu, voimassaoleva laki. Teoriaosuuden pääasialliset lähteet ovat Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta COM(2012) 11 final (myöhemmin työssä tietosuoja-asetus ja lähdeviittauksissa COM(2012)11 final), Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (jäljempänä henkilötietodirektiivi) sekä henkilötietolaki 22.4.1999/523. Lisäksi lähteinä käytetään kyseisten säädösten valmisteluasiakirjoja, oikeuskirjallisuutta sekä oikeustapauksia. Työ keskittyy käsittelemään lähinnä tietosuoja-asetuksen kolmatta ja neljättä lukua, joissa käsitellään rekisteröidyn oikeuksia sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia. Lisäksi tietosuoja-asetuksen ensimmäisestä ja toisesta luvusta, joissa kerrotaan käsittelyn yleisistä säännöksistä ja periaatteista, nostetaan esille tärkeimpiä säädöksiä.

Työn haastatteluosuudessa pyritään teemahaastattelun avulla selvittämään, miten asetus vaikuttaa Oamkissa ja miten organisaatio on varautunut asetuksen tuomiin muutoksiin. Koska oikeustradenomin opinnoissa painotetaan käytännönläheisyyttä, myös opinnäyte lähestyy aihetta käytännön näkökulmasta: mitkä ovat ne konkreettiset asiat, jotka tulevat muuttumaan Oamkissa.

Kiinnostus tietosuojaan syntyi harjoittelujakson aikana Suomen suurlähetystössä Tukholmassa, missä henkilötietoja käsiteltiin työtehtävien puitteissa päivittäin. Aluksi ajatuksena oli tutkia suurlähetystön toimintaa säätelevää lainsäädäntöä ja tehdä vertailua Suomen ja Ruotsin

henkilötietolakien välillä. Aihe muokkautui kuitenkin käytännön syistä tutkailemaan EU:n lainsäädäntöuudistusta. Työn toimeksiantajaksi löytyi Oulun ammattikorkeakoulu opettajan ehdotuksesta.

Opinnäytetyön pääluku kaksi käsittelee tietosuojaa yleisesti, siinä kerrotaan lyhyesti tietosuojan historiasta ja sen kehityksestä sekä selitetään tietosuojalainsäädännön yleisimpiä käsitteitä henkilötietolain mukaan. Jos henkilötietolain ja tietosuoja-asetuksen määritelmät käsitteistä eroavat, esitetään myös tietosuoja-asetuksessa annettu määritelmä. Kolmannessa pääluvussa esitellään toimeksiantajaorganisaatio, Oulun ammattikorkeakoulu Oy. Neljäs pääluku käsittelee tietosuoja-asetusta, verraten sen säädöksiä nykyiseen lainsäädäntöön. Pääpaino on rekisteröidyn oikeuksia ja rekisterinpitäjän velvollisuuksia koskevissa tietosuoja-asetuksen kolmannessa ja neljännessä luvussa. Työn viidennessä pääluvussa käsitellään teemahaastatteluissa esiin nousseita asioita.

2 TIETOSUOJA

Henkilötietojen suoja ja tietosuoja eivät ole käsitteinä synonyymeja, vaikka ne usein sekoitetaan, sillä tietosuoja voi koskea myös yritystietoja. Kuitenkin henkilötietojen suojaan liittyvät periaatteet ovat samoja kuin tietosuojan vaatimukset, ja Neuvosen mukaan henkilötietojen suoja toteutetaan noudattamalla näitä periaatteita ja turvaamalla tietosuojan riittävyys henkilötietojen käsittelyssä. (Neuvonen 2014, 64.)

Henkilötietojen suoja on perusoikeuksiin kuuluvan yksityisyyden suojan osa-alue ja niiden suojaaminen perustuu perustuslakiin, jonka mukaan jokaisella on oikeus turvattuun yksityiselämään, kunniaan ja kotirauhaan. Samassa pykälässä todetaan, että henkilötietojen suojaamisesta säädetään tarkemmin lailla. (Suomen perustuslaki 11.6.1999/731, 10 §.)

2.1 Tietosuojalainsäädännön kehitys

Ajatus yksityisyydestä oikeutena on lähtöisin Yhdysvalloista, jossa 1800-luvun lopulla lehdistö raportoi kansalaisten yksityiselämästä julkisesti. Vastalauseena tälle kaksi lakimiestä kirjoitti artikkelin The Right to Privacy, jossa korostettiin ajatusta the right to be alone – oikeus olla yksin tai omassa rauhassa. (Korhonen 2003, 79-80.) Korhonen viittaa myös Saarenpäähän, joka muistuttaa, että keskustelua oikeudellisesta yksityisyydestä on käyty jo paljon aiemmin, esimerkiksi Platonin ja John Stuart Millin kirjoituksissa.

Yhdistyneiden kansakuntien vuoden 1948 Ihmisoikeuksien yleismaailmallisen julistuksen myötä YK:n jäsenmaat sitoutuivat yhteistyössä edistämään ihmisoikeuksia. Julistus oli ensimmäinen asiakirja, jossa ihmisoikeudet oli koottu yhteen. Nykyisin nämä oikeudet ovat osana demokraattisten valtioiden perustuslakeja. (United for Human Rights 2014, viitattu 8.1.2015.) Julistuksen 12. artiklan mukaan kenenkään yksityiselämään ei saa mielivaltaisesti puuttua eikä mainetta tai kunniaa loukata, ja jokaisella on lain suoja tällaista loukkausta vastaan (United Nations Human Rights 2015, viitattu 8.1.2015).

Ihmisoikeuksien yleismaailmallisen julistuksen pohjalta säädetty Euroopan ihmisoikeussopimus tuli voimaan 1953. Euroopan ihmisoikeustuomioistuin valvoo sopimuksen noudattamista, ja antaa

pyydettyäessä tuomioita ihmisoikeuksien toteutumiseen liittyvissä riitatilanteissa. (Suomen ulkoasiainministeriö 2015, viitattu 8.1.2015.) Sopimuksen 8 artiklan mukaisesti jokaisella on oikeus nauttia yksityis- ja perhe-elämän kunnioitusta, johon viranomaiset voivat puuttua vain lain niin salliessa (Euroopan ihmisoikeussopimus 2015, viitattu 1.12.2014).

Henkilötietojen siirtämiseen maiden välillä ryhdyttiin kiinnittämään huomiota 1970-luvulta alkaen, ja OECD:n tietoturvasuositus (1980) sisälsikin tietoturvaan, kansainväliseen tiedonsiirtoon, rekisteröidyn oikeuksiin ja henkilötietojen keräämiseen liittyviä periaatteita. Samanaikaisesti valmistellussa Euroopan neuvoston tietosuojasopimuksessa (1981) määritellään perusperiaatteet, joihin sopimuksen hyväksyneet osapuolet sitoutuvat yksityisyyden suojaamiseksi henkilötietojen automaattisessa tietojenkäsittelyssä. (HE 96/1998 vp, Yleisperustelut, jakso 2, Kansainvälinen kehitys & Korhonen 2003, 93.)

Henkilörekisterilalla (471/1987) toteutettiin tietosuojasopimuksen asettamat vaatimukset Suomen lainsäädännössä. Samalla tavoitteeksi muodostui ennaltaehkäistä henkilötietojen käytön kautta tapahtuva yksityisyyden suojan loukkaus. Laissa säädettiin muun muassa vaatimukset tietojen keräämisen asianmukaisuudesta ja laillisuudesta, rekisterinpidon edellytyksistä sekä rekisteröidyn oikeuksista. (HE 96/1998 vp, Yleisperustelut, jakso 2, Henkilörekisterilaki.)

EU:n henkilötietodirektiivillä 95/46/EY yhtenäistettiin lainsäädäntöä, ja sen tavoitteina oli yksilöiden perusoikeuksien ja -vapauksien turvaaminen ja henkilötietojen vapaan liikkuvuuden turvaaminen EU:n sisällä. Direktiivin pohjalla olivat OECD:n tietosuojasuositus ja Euroopan neuvoston tietosuojasopimus, mutta direktiivi tarkensi ja lisäsi vaatimuksia tietoja siirrettäessä maiden välillä sekä laajensi rekisteröidyn oikeuksia. (HE 96/1998 vp, Yleisperustelut, jakso 1, Johdanto.) Direktiivin pohjalta säädettiin henkilötietolaki 22.4.1999/523, jossa henkilörekisterilakiin verrattuna säädeltiin tarkemmin arkaluontoisten tietojen ja henkilötunnuksen käyttöä (HE 96/1998 vp, & Pitkänen ym. 2013, 112.)

Nizzan huippukokouksessa 2000 hyväksytyn Euroopan unionin perusoikeuskirjan 7 & 8 artiklat suojaavat yksityis- ja perhe-elämää sekä takaavat jokaiselle oikeuden henkilötietojensa suojaan (Euroopan unionin perusoikeuskirja 2015, viitattu 15.4.2015). Alun perin lähinnä julistuksen tasoisesta perusoikeuskirjasta tuli oikeudellisesti sitova Lissabonin sopimuksen (2009) myötä (Eurooppatiedotus 2015, viitattu 24.3.2015.)

2.2 Yleiset käsitteet

Tavallisimmat käsitteet esitellään tässä henkilötietolain pohjalta. Jos tietosuoja-asetus määrittelee käsitteen erilailla, myös sen säädökset esitetään.

Henkilötieto määritellään henkilötietolain 22.4.1999/523 3 §:n mukaan

1) kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Henkilötiedon käsitteen kannalta ei ole merkitystä, missä muodossa, millä tavalla tai millaiselle alustalle tiedot on tallennettu. Henkilötieto voi olla tekstin lisäksi esimerkiksi valokuva tai graafinen kuvio. Henkilötietona pidetään henkilötunnuksen, kotiosoitteen tai potilastietojen kaltaisten tietojen lisäksi auton rekisterinumeron tai tietokoneen IP-osoitetta, jos henkilö on yksilöitävissä näiden perusteella. (Pitkänen ym. 2013, 42, 44, 47.) Rekisteröity on henkilö, jota henkilötieto koskee (HeTiL 3.5 §).

Tietosuoja-asetuksessa henkilötieto määritellään rekisteröidyn käsitteen kautta. Rekisteröity on luonnollinen henkilö, joka voidaan tunnistaa suoraan tai epäsuorasti kohtuuden rajoissa olevin keinoin esimerkiksi henkilönumeron tai jonkin fyysisen, geneettisen tai taloudellisen, henkilölle tunnusomaisen, tekijän avulla. (COM(2012)11 final, 4 artikla 1 alakohta.) Henkilötietoja ovat kaikki rekisteröityyn liittyvät tiedot (COM(2012)11 final, 4 artikla 2 alakohta).

Henkilörekisteri muodostuu automaattisen tietojenkäsittelyn avulla käsiteltävästä, yhteenkuuluvista merkinnöistä koostuvasta tietojoukosta. Myös kortistoa, luetteloa tai muulla tavoin järjestetty tietojoukkoa pidetään henkilörekisterinä, jos tiettyä henkilöä koskeva tieto on löydettävissä helposti. (HeTiL 3.3 §.) Vaikka jokin automaattisen tietojenkäsittelyn avulla laadittu asiakirja, kuten muistio tai luettelo, sisältää henkilötietoja, se ei automaattisesti ole henkilörekisteri. Hallituksen esityksessä 96/1998 viitataan tietosuojalautakunnan päätökseen (n:o 7/26.3.1990), jonka mukaan automaattisen tietojenkäsittelyn avulla laadittu henkilötietoja sisältävä luettelo ei ole henkilörekisterilain mukainen automaattisen tietojenkäsittelyn avulla ylläpidettävä henkilörekisteri. Valmistelutöissä edellytetään, ettei tällaista asiakirjaa pysyvämmiin säilytetä sähköisenä tiedostona osana tietojenkäsittelyjärjestelmää. (HE 96/1998, Yksityiskohtaiset perustelut, 1 luku Yleiset säännökset.)

Tietosuoja-asetuksessa käytetään henkilörekisterin sijasta termiä rekisteröintijärjestelmä. Sillä tarkoitetaan järjestettyjä henkilötietojen kokoelmia, jotka voivat olla keskitettyjä, hajautettuja tai jollain perustein jaettu, ja joista tiedot ovat saatavilla tietyin perustein. (COM(2012)11 final, 4 artikla 4 alakohta.)

Henkilötietojen käsittelyllä tarkoitetaan kaikkia henkilötietoihin kohdistuvia toimenpiteitä, kuten keräämistä, tallettamista, siirtämistä ja luovuttamista (HeTiL 3.2 §). Henkilötietolain 8 §:ssä käsittelyn yleiseksi edellytykseksi määritellään, että henkilötietoja saa käsitellä vain rekisteröidyn yksiselitteisestä suostumuksesta tai toimeksiannosta, tai sopimuksen, jossa rekisteröity on osallisena, täytäntöönpanemiseksi. Yksittäistapauksissa tietojen käsittely on sallittu rekisteröidyn elintärkeän edun suojaamiseksi. Hallituksen esityksessä nostetaan esimerkiksi rekisteröidyn hengen tai terveyden pelastaminen, kun se edellyttää tietojen käsittelyä eikä suostumusta ole mahdollista saada (HE 96/1998, Yksityiskohtaiset perustelut, 2 luku, Henkilötietojen käsittelyä koskevat yleiset periaatteet). Tietoja saa käsitellä myös, jos käsittely kuuluu rekisterinpitäjän lain mukaisiin velvollisuuksiin, rekisteröidyllä on asiallinen yhteys rekisterinpitäjän toimintaan (asiakas- tai palvelusuhde tai jäsenyys) tai jos käsitellään konsernin tai muun taloudellisen yhteenliittymän asiakkaiden tai työntekijöiden tietoja kyseisen yhteenliittymän sisällä. (HeTiL 8 §).

Henkilötietolain valmisteluasiakirjoissa määritellään suostumus vapaaehtoiseksi, yksilöidyksi ja tietoiseksi tahdonilmaukseksi, jolla rekisteröity ilmaisee hyväksyvänsä henkilötietojensa käsittelyn. Myös suullinen suostumus on pätevä, jos se täyttää edellä mainitut vaatimukset. Rekisteröidyllä on oikeus perua suostumuksensa milloin tahansa. (HE 96/1998 vp, Yksityiskohtaiset perustelut, 1 luku, 1.1. Henkilötietolaki, 1 luku Yleiset säännökset.) Arkaluonteisia tietoja ja henkilötunnusta saa käsitellä rekisteröidyn nimenomaisella suostumuksella (HeTiL 11–12 §).

Tietosuoja-asetus lisää rekisteröidyn antaman suostumuksen määritelmään vaatimuksen tahdonilmauksen nimenomaisuudesta. Lisäksi asetus tarkentaa, että suostumus voi olla lausuma eli sanallinen, tai suostumusta ilmaiseva toimi, eli jokin teko. (COM(2012)11 final, 4 artikla 8 alakohta.) Tietosuoja-asetus rajaa käsittelyn lainmukaisuuden edellytyksiä niin, että käsittely on lainmukaista vain rekisteröidyn suostumuksella, sopimuksen täytäntöönpanoa varten, rekisterinpitäjän lakisääteisen velvoitteen toteuttamiseksi, rekisteröidyn elintärkeän edun suojaamiseksi, yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjän julkisen vallan

käyttöä varten rekisterinpitäjän oikeutetun edun toteuttamiseksi. Henkilötietolaissa mainittu asiallinen yhteys, esimerkiksi jäsenyys, tai konsernin sisällä asiakkaiden tai työntekijöiden henkilötietojen käsittely, ei ole tietosuoja-asetuksen mukainen laillinen edellytys henkilötietojen käsittelylle. (COM(2012)11 final, 6 artikla 1 alakohta.)

Tietosuoja-asetus pyrkii suojelemaan erityisesti lapsia ja heidän henkilötietojaan. Asetuksen 8 artiklassa säädetäänkin, että tietoyhteiskunnan palveluja tarjottaessa suoraan alle 13-vuotiaalle, henkilötietojen käsittelyyn tarvitsee vanhemman tai huoltajan suostumuksen tai valtuutuksen, muuten käsittely on lainvastaista. Rekisterinpitäjän vastuulla on kohtuullisin toimenpitein toteutettava suostumuksen saaminen. (COM(2012)11 final, 8 artikla.)

Rekisterinpitäjä on henkilö, yhteisö, laitos tai säätö, jonka käyttöä varten henkilörekisteri perustetaan, jolla on oikeus määrätä sen käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. Rekisterinpitäjiä voi olla yksi tai useampia. (HeTiL 3.4 §.) Tietosuoja-asetuksen mukainen rekisterinpitäjä on se toimija, joka määrittelee henkilötietojen käsittelyn tarkoitukset, edellytykset ja keinot (COM(2012)11 final, 4 artikla 5 alakohta).

Rekisteriseloste on jokaisen saatavilla oleva asiakirja, jonka rekisterinpitäjä laatii henkilörekisteristä. Siinä täytyy käydä ilmi rekisterinpitäjän sekä mahdollisesti tämän edustajan nimi ja yhteystiedot, missä tarkoituksessa henkilötietoja käsitellään, kuvaus rekisteröidyistä ryhmistä, tiedot siitä mihin tietoja luovutetaan ja luovutetaanko niitä EU:n tai Euroopan talousalueen ulkopuolelle, sekä pääsääntöinen kuvaus miten rekisteriä suojataan. (HeTiL 2:10 §.) Tietosuoja-asetus ei mainitse rekisteriselostetta lainkaan, mutta asetuksen 11 artiklassa rekisterinpitäjää veloitetaan toimittamaan rekisteröidylle vastaavat tiedot kuin rekisteriselosteessa vaaditaan (COM(2012)11 final, 11 artikla).

Tietosuoja-asetuksen 28 artikla säättää rekisteriseloste-nimikkeen sijaan asiakirjoista, jotka rekisterinpitäjän, henkilötietojen käsittelijän sekä rekisterinpitäjän edustajan täytyy vastuullaan tapahtuvista tietojenkäsittelytoimista säilyttää. Asiakirjoissa täytyy ilmetä rekisterinpitäjän, tämän edustajan, yhteisen rekisterinpitäjän taikka henkilötietojen käsittelijän nimi yhteystietoineen sekä mahdollisen tietosuojavastaavan yhteystiedot, henkilötietojen käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja tiedot henkilötietojen vastaanottajista sekä tarvittaessa tietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle sekä maininta eri tietoryhmien poistamisen määräaajoista. (COM(2012)11 final, 28 artikla).

Huolellisuusvelvoite tarkoittaa, että henkilötietoja täytyy käsitellä laillisesti noudattaen huolellisuutta ja hyvää tiedonkäsittelytapaa (HeTiL 2:5 §). Hyvän tietojenkäsittelytavan mukaisesti rekisteröidyn oikeudet otetaan huomioon ja tietojenkäsittelyllä käsitellään vain käyttötarkoitukseen nähden tarpeellisia henkilötietoja (Voutilainen 2012, 41). Tietosuoja-asetuksen mukaan tietoja täytyy käsitellä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (COM(2012)11 final, 5 artikla 1a kohta).

Henkilötietolain 6 §:n mukaisesti henkilötietojen käsittelyn täytyy olla rekisterinpitäjän toiminnan kannalta asiallisesti perusteltua, ja käsittelyn tarkoitus täytyy määritellä ennen tietojen hankkimista. Myös tietojen hankintatapa täytyy ilmaista. Lain 7 §:ssä määritellyn käyttötarkoitussidonnaisuuden mukaan henkilötietojen käsittelylle on aina oltava peruste, ja niitä saa käyttää ainoastaan siihen tarkoitukseen, jota varten ne on kerätty. Tarpeellisuusvaatimuksella tarkoitetaan, että vain määritellyn käsittelyn perustelun kannalta tarpeellisia tietoja saa kerätä ja käsitellä, ja virheettömyysvaatimuksen mukaisesti virheellisten, epätäydellisten tai vanhentuneiden tietojen käsittely ei ole sallittu. (HeTiL 2:6-7, 2:9.)

Tietosuoja-asetuksen 5 artiklassa käyttötarkoitussidonnaisuus ja tarpeellisuusvaatimus ilmaistaan niin, että tietoja saa kerätä tiettyyn nimenomaiseen ja lailliseen tarkoitukseen, ja niiden täytyy olla olennaisia, asianmukaisia ja niiden määrä rajoitettava mahdollisimman vähään käsittelytarkoitukseen nähden. Tietojen käsittely myöhemmin vastoin alkuperäistä tarkoitusta on kielletty. Virheettömyysvaatimus määrittää siten, että tietojen on oltava täsmällisiä ja päivitettyjä ja virheelliset tiedot on poistettava tai oikaistava viipymättä. (COM(2012)11 final, 5 artikla 1b-d kohdat.)

Arkaluonteisilla tiedoilla tarkoitetaan tietoja, joilla kuvataan esimerkiksi rotua, poliittista tai muuta vakaumusta, terveydentilaa tai sosiaalihuollon tarvetta. Näiden tietojen käsittely on pääsääntöisesti kielletty. Käsittely sallitaan ainoastaan henkilötietolain 12 §:ssä määritellyin poikkeuksin, joihin kuuluu muun muassa rekisteröidyn nimenomainen suostumus, käsittelyn tarpeellisuus rekisteröidyn tai muun henkilön elintärkeän edun suojaamiseksi rekisteröidyn ollessa estynyt antamaan suostumusta, tietojenkäsittelystä säädettäessä laissa taikka tietosuojalautakunnan myöntämä käsittelylupa. Heti, kun peruste arkaluonteisen tiedon käsittelylle poistuu, tiedot on poistettava rekisteristä välittömästi. (HeTiL 11-12 §.)

Tietosuoja-asetuksessa arkaluonteisten tietojen, tai kuten 9 artiklan otsikossa muotoillaan, erityisten tietoryhmien, käsittely on kielletty. Poikkeukset käsittelykieltoon ovat pitkälti samanlaiset kuin henkilötietolaissa (COM(2012)11 final, 9 artikla.)

Henkilötunnuksen käsittely on sallittu rekisteröidyn yksiselitteisellä suostumuksella, käsittelystä säädettyä laista taikka jos rekisteröity täytyy yksilöidä esimerkiksi laissa säädetyn tehtävän suorittamiseksi taikka rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi. Henkilötunnusta ei saa turhaan merkitä esimerkiksi tulostettuihin asiakirjoihin. (HeTiL 13 §.) Henkilötunnuksen käytöstä tietosuoja-asetus ei säädä erikseen.

Henkilötietolain 12 §:n mukaan yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista koskevien tietojen käsittely on sallittu, kun rekisteröity itse tuo tiedot julkiseksi (HeTiL 12 § 1.2). Tietosuoja-asetus laajentaa tämän poikkeuksen koskemaan kaikkia arkaluonteisia tietoja (COM(2012)11 final, 9 artikla 2e kohta).

Tietosuoja-asetuksessa määritellään uusina periaatteina läpinäkyvyyssperiaate, tietojen minimoinnin periaate sekä rekisterinpitäjän kattavan vastuun vahvistaminen. Näitä käsitellään pääluvussa 4.

3 OAMK

Oulun ammattikorkeakoulu on Oulussa ja Oulaisissa toimiva kolmannen asteen oppilaitos, jossa on noin 8500 opiskelijaa, ja henkilöstöä 640 (Oulun ammattikorkeakoulu 2015a, viitattu 1.4.2015). Vuoden 2015 yhteishaussa Oamkissa on yli 1600 aloituspaikkaa (Oulun ammattikorkeakoulu 2015b, viitattu 24.3.2015) 28 koulutusohjelmassa, joista kolme on englanninkielisiä, kulttuurin, liiketalouden, luonnonvara-alan, sosiaali- ja terveysalan ja tekniikan aloilla. Lisäksi ylempään AMK-tutkintoon johtavaa koulutusta annetaan neljässä koulutusohjelmassa sekä tarjotaan ammatillisen opettajakorkeakoulun ja avoimen AMK:n opetusta (Oulun ammattikorkeakoulu 2015a, viitattu 24.3.2015).

3.1 Organisaatio

Vuoden 2014 ammattikorkeakoululain 14.11.2014/932 myötä Oamkista tuli osakeyhtiömuotoinen oikeushenkilö, jonka toimielimiä ovat osakeyhtiölain mukaisesti yhtiökokous ja hallitus. Oulun kaupunki omistaa Oamkista 76,4 %, muina omistajina ovat Hailuodon, Iin, Kempeleen, Limingan, Lumijoen, Muhoksen ja Tyrnävän kunnat sekä Raahen kaupunki. (Oulun ammattikorkeakoulu 2015d, 6, viitattu 8.5.2015.) Hallituksessa on 7-9 jäsentä, jotka edustavat monipuolisesti yhteiskuntaelämän ja ammattikorkeakoulun tehtäviin liittyvää asiantuntemusta, lisäksi henkilöstöllä ja opiskelijoilla on oma edustajansa. Hallitus päättää muun muassa toiminnan ja talouden tavoitteista ammattikorkeakoululain mukaisesti. (Oulun ammattikorkeakoulu 2015c, viitattu 24.4.2015.)

Oulun ammattikorkeakoulun rehtori toimii osakeyhtiön toimitusjohtajana. Toimitusjohtajan tehtäviin kuuluu yhtiön juoksevan hallinnon hoitaminen hallitukselta saamiensa ohjeiden mukaisesti (Osakeyhtiölaki 21.7.2006/624 17 §). Ammattikorkeakoululaki lisää rehtorin tehtäviin toiminnan johtamisen ja koulua koskevista asioista päättämisen, mikäli niitä ei ole säädetty muun toimielimen tehtäviksi. Rehtorilla on vastuu ammattikorkeakoulun tehtävien hoitamisesta taloudellisesti, tehokkaasti ja tuloksellisesti, ja hän päättää myös henkilöstön ottamisesta ja irtisanomisesta sekä vastaa hallituksessa käsiteltävien asioiden valmistelusta, esittelystä ja täytäntöönpanosta. (Ammattikorkeakoululaki 18.1 §.) Rehtorin alaisuudessa toimivat korkeakoulupalvelut, joita johtaa vararehtori, koulutusosastot, henkilöstö-, viestintä- ja

talousosastot sekä kirjasto. Oamkin organisaatio uudistui syksyllä 2015, jolloin vanha yksikköjärjestelmä purettiin ja uudenlainen koulutusosastoihin perustuva järjestelmä otettiin käyttöön.

OULUN AMMATTIKORKEAKOULU :: oamk.fi



Hyväksytty hallituksessa 8.6.2015

KUVIO 4. Oamkin organisaatio 8.6.2015 (Oulun ammattikorkeakoulu 2015e, viitattu 31.8.2015)

3.2 Tietosuoja Oamkissa

Ammattikorkeakoululain mukaisesti henkilötietojen käsittelyyn ammattikorkeakouluissa sovelletaan henkilötietolakia. Arkaluonteiset tiedot täytyy säilyttää erillään muista henkilötiedoista, ja ne täytyy poistaa välittömästi kun lakisääteistä perustetta niiden säilyttämiselle ei ole, kuitenkin viimeistään neljän vuoden kuluttua tietojen merkitsemisestä rekisteriin. Koulun täytyy määrittellä tehtävät, joihin sisältyy arkaluonteisten tietojen käsittelyä, ja vain henkilöt, jotka valmistelevat tai tekevät päätöksen opiskelijavalinnasta, opiskeluoikeuden peruuttamisesta, opiskeluoikeuden palauttamisesta tai kurinpidosta taikka antavat lausuntoja kyseisistä asioista saavat käsitellä opiskelijaksi pyrkivän tai opiskelijan terveydentilaa koskevia tietoja. Rikosrekisteritietoja saavat käsitellä vain opiskeluoikeuden peruuttamista valmistelevat tai siitä päättävät henkilöt. (Ammattikorkeakoululaki 40 §.)

4 TIETOSUOJA-ASETUS

4.1 Taustaa

Vuonna 2007 hyväksytyssä Lissabonin sopimuksessa EU:n perusoikeuskirjasta tehtiin oikeudellisesti sitova, eli sille annettiin sama oikeudellinen arvo kuin unionin perussopimuksilla. Perusoikeuskirjan 7 ja 8 artikloissa säädetään, että jokaisella on oikeus yksityis- ja perhe-elämänsä, kotinsa sekä viestiensä kunnioitukseen ja henkilötietojensa suojaan. (U 21/2012 vp, 3.) Eurooppa-neuvosto hyväksyi 11.2.2009 Tukholman ohjelman (2010/C 115/01), jossa todetaan että oikeus yksityisyyteen turvataan EU:n perusoikeuskirjassa, ja unionin täytyy edistää tietosuojaa varmistamalla, että Euroopan neuvoston tietosuojasopimuksen periaatteet toteutuvat. Ohjelmassa kehoitetaan komissiota ”arvioimaan tietosuojaa koskevien eri välineiden toimivuutta ja tekemään tarvittaessa uusia lainsäädäntö- ja muita aloitteita edellä mainittujen periaatteiden tosiasiallisen soveltamisen turvaamiseksi”. (Eurooppa-neuvosto 2010, 10–11.)

Komissio valmisti lainsäädännön muutosta muun muassa konsultoimalla henkilötietodirektiivin 29 artiklan mukaista, kansallisista tietosuojaviranomaisista koostuvaa työryhmää, sekä kuuli kansalaisten mielipiteitä eurobarometrikyselyssä. Komissio antoi 25.1.2012 ehdotukset yleisestä tietosuoja-asetuksesta (COM(2012)11 final) ja direktiiviksi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta (COM(2012)10 sekä tiedonannon ”Yksityisyydensuoja verkottuvassa maailmassa” (COM(2012)09 final) Euroopan uudeksi tietosujakehykseksi. Tiedonannossa todetaan, että henkilötietoja kerätään yhä enemmän teknologian kehityksen ja globalisoitumisen myötä, ja myös keinot henkilötietojen käsittelyssä ja siirtämisessä ovat muuttuneet. Korkeatasoisella tietosuojalla pyritään edistämään yksilöiden oikeutta valvoa henkilötietojaan sekä parantamaan luottamusta onlinepalveluihin. (U 21/2012 vp, 2-3.) Tietosuojuudistuksen tavoitteena on vähentää byrokraattisia esteitä asettamalla kaikkien jäsenmaiden toimijat samojen sääntöjen ääreen, jolloin komission tavoite digitaalisten sisämarkkinoiden kehittämisestä helpottuu (European Commission 2015a, viitattu 16.4.2015).

Tietosuoja-asetuksen perusteluissa mainitaan Euroopan unionista tehdyn sopimuksen toissijaisuusperiaate, jonka mukaan unionin tasolla toimitaan ainoastaan silloin, kun jäsenvaltiot eivät itsenäisesti voi saavuttaa suunniteltuja tavoitteita, vaan toiminnan laajuuden vuoksi ne

saavutetaan helpommin unionin tasolla. Direktiivimuotoinen säätely saattaa aiheuttaa tietosuojan tason vaihtelun jäsenvaltioissa ja koska henkilötietoja siirretään valtioiden rajojen yli yhä enemmän, on yksilöiden edun mukaista rakentaa yhtenäinen kehys, asetusmuotoinen tietosuojasäätely, henkilötietojen suojaksi. (COM(2012)11 final, 6.) Tämä asia on tullut esille kirjoituksissa Henkilötietodirektiivistä:

Kansallisia säädöksiä valmisteltaessa on kuitenkin vaikeuksia aiheuttanut tulkinta siitä, mitkä direktiivin säännökset ovat ehdottoman sitovia ja mitkä taas enemmän mukailtavissa kansallisella tasolla. Tämän vuoksi myös pohjoismaisissa henkilötietosäädöksissä on joitain eroja ja ne eivät ole täysin identtisiä keskenään (Korhonen 2003, 95.)

Asetusehdotuksessa todetaankin, ettei Henkilötietodirektiivillä olla pystytty estämään henkilötietojen suojan hajanaisuutta tai parantamaan kuluttajien luottamusta verkkoympäristössä tehtyihin toimintoihin. Vahvalla tietosuojasäännöksellä pyritään siihen, että niin yksilöt, viranomaiset kuin talouden toimijat voivat luotaa digitaalimarkkinoiden turvallisuuteen ja tehokkuuteen. (COM(2012)11 final, 2.)

Tietosuoja-asetusehdotus käsitellään tavallisessa lainsäätämisyjärjestyksessä, eli parlamentin ja neuvoston yhteistyössä. Parlamentti hyväksyi kansalaisvapauksien sekä oikeus- ja sisäasioidenvaliokunnan mietinnön asetusehdotuksesta maaliskuussa 2014. (Eduskunta 2015, viitattu 12.3.2015.) Asetuksen käsittely eteni neuvostolle, ja unionin oikeus- ja sisäasioiden neuvosto (OSA) käsitteli asiaa kokouksessaan 12.–13.3.2015 tarkoituksenaan päästä yksimielisyyteen asetuksen 2., 6. & 7. luvuista (Euroopan unionin neuvosto 2015a, viitattu 12.3.2015). Kokouksissaan loka- ja joulukuussa 2014 neuvosto keskusteli muun muassa oikeudesta tulla unohdetuksi sekä hyväksyttiin osittaiset yleisnäkemykset asetuksen alueellisesta soveltamisalasta, rekisterinpitäjien ja tietojenkäsittelijöiden velvollisuuksista sekä tiedonsiirrosta kolmansiin maihin (Euroopan unionin neuvosto 2015b, viitattu 12.3.2015). Kokouksessa 15.6.2015 neuvosto pääsi yleisnäkemykseen asetuksesta, ja 24.6.2015 aloitettiin kolmikantaneuvottelut Euroopan parlamentin ja neuvoston välillä. Komissio odottaakin neuvoston ja parlamentin pääsevän täydelliseen yhteisymmärrykseen viimeistään vuoden 2015 loppuun mennessä. Virallisesti asetus hyväksyttäneen vuoden 2016 alkupuolella, jolloin kahden vuoden siirtymäaika alkaa. (European Commission 2015a, viitattu 16.4.2015 & European Commission 2015d, viitattu 31.8.2015.)

4.2 Rekisterinpitäjän velvollisuudet

Tietosuoja-asetuksen tavoitteena on tehdä rekisterinpitäjistä tilivelvollisia toiminnastaan ja tietojen suojaamisesta oletusarvoista. Tietosuoja otetaan lähtökohdaksi myös uusien ohjelmien ja palvelujen suunnittelussa. Uudeksi velvollisuudeksi asetuksessa määrätään vaikutustenarviointi, joka on tehtävä, jos tietojenkäsittelyn luonne sitä vaatii. Asetuksen myötä velvollisuus ilmoittaa tietovuodoista laajenee sekä tietosuojarikkomuksista seuraa sanktio, joita ei aiemmassa lainsäädännössä ole ollut. Rekisterinpitäjän lisäksi vastuu henkilötietojen käsittelystä voi asetuksen myötä olla myös henkilötietojen käsittelijällä. Tietyissä tilanteissa rekisterinpitäjän täytyy nimittää tietosuojavastaava, jonka tehtäviin kuuluu neuvoa ja valvoa tietosuoja-asetuksen noudattamista.

4.2.1 Yleiset velvollisuudet

Rekisterinpitäjän täytyy noudattaa toiminnassaan henkilötietojen käsittelyä koskevia periaatteita, eli hyvää tiedonkäsittelytapaa. Näihin periaatteisiin kuuluu muun muassa tietojen käsittely lainmukaisesti ja asianmukaisesti, tietojen kerääminen nimenomaista ja laillista tarkoitusta varten, tietojen täsmällisyys ja päivittäminen sekä virheellisten tietojen oikaiseminen tai poistaminen. Tietosuoja-asetuksessa esitetään uusi periaate, läpinäkyvyys, jonka mukaan tietojenkäsittelyn on tapahduttava rekisteröidyn kannalta läpinäkyvästi (COM(2012)11 final, 5 artikla). Henkilötietodirektiiviin verrattuna tietosuoja-asetus täsmentää ja tiukentaa tietojenkäsittelyn periaatteita: direktiivissä todetaan, etteivät tiedot saa olla liian laajoja tarkoitukseen nähden (Henkilötietodirektiivi 6 artikla c). Sama asia ilmaistaan asetuksessa niin, että tietojen määrä on rajoitettava mahdollisimman vähään (COM(2012)11 final, 5 artikla c-kohta). Tätä kutsutaan tietojen minimoinnin periaatteeksi.

Tietosuoja-asetus luo rekisterinpitäjälle uuden tilivelvollisuuden periaatteen toiminnastaan. 22 artiklan mukaisesti asetuksen noudattaminen, eli hyväksytyt toimintamenetelmät ja toteutetut toimenpiteet, on pystyttävä osoittamaan. Rekisterinpitäjän, henkilötietojen käsittelijän ja rekisterinpitäjän edustajan on lähtökohtaisesti säilytettävä tietojenkäsittelytoimia koskevat keskeiset asiakirjat (Tietosuojaytöryhmä 2012, 16.) Kyseisessä artiklassa mainitaan 28 artiklassa määriteltyjen asiakirjojen säilyttäminen, tietoturvasuoritusvaatimusten täytäntöönpano (30 artikla), tietosuoja koskevan vaikutustenarvioinnin laatiminen (33 artikla), valvontaviranomaisen

ennakkohyväksynnän tai -kuulemisen vaatimusten noudattaminen (34 artikla, kohdat 1 ja 2) tietosuojavaastaavan nimittäminen (35 artikla). (COM(2012)11 final 22 artikla.)

4.2.2 Sisäänrakennettu ja oletusarvoinen tietosuoja sekä tietoturvallisuus

Tietosuoja-asetuksen 23 artiklan sisäänrakennetulla ja oletusarvoisella tietosuojalla tarkoitetaan, että tietosuoja-vaatimukset täyttyvät jo tuotteiden tai palvelujen suunnitteluvaiheessa, ja näiden oletusasetukset ovat yhdenmukaisia tietosuoja-asetuksen kanssa. Rekisterinpitäjän on varmistettava tämä käyttäen asianmukaisia teknisiä ja organisatorisia toimenpiteitä sekä uusinta tekniikkaa, ja varmistettava että oletusarvoisesti käsitellään vain välttämättömiä henkilötietoja. Tietoja ei kerätä tai säilytetä enempää tai kauempaa kuin on välttämätöntä. (COM(2012)11 final, 28.)

Tietosuoja-asetuksen 30 artiklassa rekisterinpitäjän ja henkilötietojen käsittelijän täytyy varmistaa asianmukaisin teknisin ja organisatorisin toimenpitein asianmukainen turvallisuustaso. Tietoturvallisuudesta tehdyn riskienarvioinnin pohjalta tehtävät toimenpiteet henkilötietojen suojaamiseksi vahingossa tai tahallisesti tapahtuvalta tuhoamiselta, häviämiseltä, lainvastaisen käsittelyn, luvattoman luovuttamisen, levittämisen, tiedonsaannin tai tietojen muuttamisen estämiseksi on toteutettava toimenpiteiden toteuttamiskustannukset ja uusin tekniikka huomioon ottaen. (COM(2012)11 final, 30 artikla.)

Henkilötietodirektiivin 17 artikla asettaa rekisterinpitäjälle vastuun varmistaa käsittelyn turvallisuuteen liittyvät toimenpiteet. Jos rekisterinpitäjä valitsee henkilötietojen käsittelijäksi ulkopuolisen tahon, on rekisterinpitäjän huolehdittava että tarvittavat toimenpiteet toteutetaan. (Henkilötietodirektiivi, 17 artikla). Muutokset lainsäädännössä asettavat myös tietojenkäsittelijän vastuuseen käsittelyn turvallisuudesta. Aiemmin vastuu on ollut vain rekisterinpitäjällä.

4.2.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkohyväksyntä

Tietosuoja-asetus velvoittaa laatimaan arvion henkilötietojen käsittelytoimien vaikutuksesta henkilötietojen suojalle, jos niihin liittyy käsittelyn luonteen, laajuuden tai tarkoituksen vuoksi rekisteröidyn oikeuksien ja vapauksien kannalta erityisiä riskejä. Arvion tekee joko rekisterinpitäjä tai henkilötietojen käsittelijä. Esimerkiksi järjestelmälliset arvioinnit henkilökohtaisista

ominaisuuksista (esimerkiksi taloudellinen tila, mieltymykset, sijainti) oikeusvaikutuksia aiheuttavia toimenpiteitä varten sekä terveyttä, rotua tai terveydenhuollon antamista koskevat selvitykset, jos niiden tarkoituksena on toteuttaa toimenpiteitä tietyille yksilöille, sisältävät asetuksen mukaan riskejä. Lisäksi riskialttiina pidetään yleisölle avoimien alueiden valvontaa ja lasten tietojen tai geneettisiä tai biometrisiä tietoja koskevien tietojen käsittelyä suuren mittakaavan järjestelmissä.

Vaikutustenarvioinnissa täytyy esittää kuvaus suunnitelluista käsittelytoimista, arvio toimiin liittyvistä riskeistä rekisteröidyn oikeuksien ja vapauksien kannalta, puuttumistoimet riskeihin sekä ne takeet, suojatoimenpiteet ja keinot henkilötietojen suojan varmistamiseksi ja asetuksen noudattamisen osoittamiseksi. Vaikutustenarvioinnista voidaan poiketa, jos rekisterinpitäjänä toimii viranomainen tai julkishallinnon elin, ja henkilötietojen käsittely perustuu lakisääteisen velvoitteen noudattamiseen. (COM(2012)11 final, 33 artikla.)

Vaikutustenarvioinnilla korvataan henkilötietodirektiivin 18 artiklassa säädetty rekisterinpitäjän tai tämän edustajan ilmoitusvelvollisuus valvontaviranomaiselle ennen kuin kokonaan tai osittain automatisoitu henkilötietojen käsittely toteutetaan. Nykyisestä ilmoitusmenettelystä voidaan poiketa vain, jos käsittelytoimet ja käsiteltävät tiedot eivät todennäköisesti loukkaa rekisteröityjen oikeuksia ja jäsenvaltiot ovat määrittäneet käsittelyn tarkoituksen, käsiteltävät tiedot tai tietoryhmät, rekisteröityjen ryhmän tai ryhmät, tietojen vastaanottajan tai vastaanottajaryhmät ja tietojen säilyttämisaajan. Myöskään lain mukaisesta julkisesta rekisteristä ei välttämättä tarvitse tehdä ilmoitusta, eikä silloin, kun rekisterinpitäjä on nimennyt henkilötietojen suojaamisesta vastaavan henkilön, joka huolehtii direktiivin säädösten noudattamisesta. (Henkilötietodirektiivi 18 artikla.)

Asetuksen 34 artiklan mukaan rekisterinpitäjän tai henkilötietojen käsittelijän on saatava henkilötietojen käsittelystä ennakko hyväksyntä ennen tietojenkäsittelyn aloittamista, kun kyseessä on henkilötietojen siirtäminen kolmanteen maahan tai kansainväliselle järjestölle, ja rekisterinpitäjä ei saa asianmukaisia takeita henkilötietojen suojaamisesta. Jos tietosuojaa koskevassa vaikutustenarvioinnissa käy ilmi, että henkilötietojen käsittelytoimiin liittyy merkittäviä erityisiä riskejä, valvontaviranomaista on kuultava ennen käsittelyä sen varmistamiseksi, että suunniteltu käsittely on asetuksen mukaista. Valvontaviranomainen voi myös suorittaa ennakko kuulemisen, jos katsoo sen tarpeelliseksi. Jos suunniteltu käsittely ei ole asetuksen

mukaista, valvontaviranomaisen täytyy kieltää suunniteltu käsittely ja esitettävä ehdotukset puutteiden korjaamiseksi.

Henkilötietodirektiivissä ennakkohyväksynnästä käytetään termiä ennakkotarkastus. Jäsenvaltioiden tulee 20 artiklan mukaisesti määrittää erityisiä riskejä mahdollisesti aiheuttavat käsittelyt ja valvottava niiden tutkimista ennen toteutusta. (Henkilötietodirektiivi 20 artikla).

4.2.4 Tietosuojavastaava

Tietosuoja-asetuksen 35 artiklassa säädetään tietosuojavastaavan nimittämisestä. Nimittäminen on pakollista, kun tietojenkäsittelijänä on viranomainen tai julkishallinnon elin, yli 250 työntekijän yritys tai kun henkilötietojen käsittelytoimet edellyttävät luonteena, laajuutensa ja/tai tarkoituksensa vuoksi rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, ja rekisterinpitäjän tai henkilötietojen käsittelijän keskeiset tehtävät muodostuvat tällaisista käsittelytoimista. Muissa tapauksissa tietosuojavastaavan nimittäminen on vapaaehtoista. Tietosuojavastaava nimitetään toimeensa vähintään kahden vuoden ajaksi, ja voidaan erottaa vain, jos ei enää täytä tehtäviensä suorittamisen edellyttämiä vaatimuksia. Tietosuojavastaavalla täytyy olla tietosuojalainsäädäntöä koskeva erityisasiantuntemus. Asetuksen 37 artiklassa määritellään tietosuojavastaavan tehtäviksi muun muassa rekisterinpitäjän tai henkilötietojen käsittelijän neuvonta tietosuoja-asetuksen niille määräämissä velvollisuuksissa, seurata henkilötietojen suojaan liittyvien toimintamenetelmien täytäntöönpanoa ja soveltamista, seurata tietosuoja-asetuksen täytäntöönpanoa ja soveltamista. (COM(2012) 11 final, 35-37 artiklat.)

Tämän hetkinen lainsäädäntö velvoittaa ainoastaan sosiaali- ja terveydenhuollon palvelun antajia, apteekkeja sekä Kansaneläkelaitosta ja Terveystieteiden tutkimuskeskusta nimittämään tietosuojavastaavan (Tietosuojavaltuutetun toimisto 2010, viitattu 30.3.2015).

4.2.5 Tietovuodot ja sanktiot

Tietosuoja-asetuksen 31 ja 32 artiklat määräävät rekisterinpitäjälle ilmoitusvelvollisuuden tietoturvaloukkaustilanteissa. Tapahtuneesta loukkauksesta on ilmoitettava tietosuojaviranomaiselle viipymättä. Jos ilmoitus tehdään yli 24 tuntia tapahtuneen jälkeen, syy viivästykseen on perusteltava. Henkilötietojenkäsittelijän täytyy ilmoittaa tietoturvaloukkauksesta

rekisterinpitäjälle heti sen tullessa ilmi. Rekisterinpitäjän täytyy ilmoituksessaan kuvata tietoturvaloukkaus ja sen mahdolliset seuraukset sekä ehdottaa tai kuvata toimenpiteet, jotka se on toteuttanut loukkauksen jälkeen ja toimenpiteet, joilla haittavaikutuksia voitaisiin lieventää. Ilmoituksessa on mainittava tietosuojavastaavan tai muun lisätietoa antavan tahon henkilöllisyys ja yhteystiedot sekä kuvata kyseisen loukkauksen kohteina olleet rekisteröityjen ryhmät ja lukumäärät. Rekisterinpitäjän on tilivelvollisuuden periaatteen mukaisesti dokumentoitava kaikki tietoturvaloukkaukseen liittyvät toimet, jotta valvontaviranomainen voi tarkistaa, että artiklaa 31 on noudatettu. (COM(2012)11 final, 31 artikla.)

Rekisteröidylle tietoturvaloukkauksesta täytyy ilmoittaa, jos loukkauksella on todennäköisiä haittavaikutuksia rekisteröidyn yksityisyyteen tai henkilötietojen suojalle. Ilmoitus täytyy antaa ilman aiheetonta viivytystä, ja siinä täytyy kuvata loukkauksen luonne ja ilmoitettava vähintään tietosuojavastaavan henkilöllisyys yhteystietoineen ja toimenpiteet, joilla lievennetään tietoturvaloukkauksen haittavaikutuksia. Ilmoitusvelvollisuudesta voidaan poiketa, jos rekisterinpitäjä osoittaa valvontaviranomaisen hyväksymällä tavalla toteuttaneensa asianmukaiset tekniset suojatoimenpiteet loukkauksen kohteena oleviin henkilötietoihin. Valvontaviranomainen voi tarvittaessa vaatia tietoturvaloukkauksen ilmoittamista rekisteröidylle, jos rekisterinpitäjä ei ole vielä sitä tehnyt ja viranomainen katsoo sen tarpeelliseksi haittavaikutusten todennäköisyyden perusteella. (COM(2012)11 final, 32 artikla.)

Henkilötietodirektiivi ja henkilötietolaki eivät säädä minkäänlaista ilmoitusvelvollisuutta tietoturvaloukkaustilanteissa. Tätä korjattiin direktiivillä 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) ja komission asetuksella 611/2013. Asetuksessa sähköisten viestintäpalvelujen tarjoajien, eli teleoperaattoreiden ja internetpalveluntarjoajien, täytyy ilmoittaa tapahtuneista tietoturvaloukkauksista viranomaiselle, ja tietyin edellytyksin myös rekisteröidylle. (Komission asetus N:o 611/2013, 1-2 artiklat.)

Tietosuoja-asetuksen 79 artiklassa määritellään sakkomaksut tilanteissa, joissa rekisterinpitäjä tai henkilötietojen käsittelijä jättää tahallaan tai tuottamuksellisesti noudattamatta asetuksen velvoitteita. Vakavimmissa rikkomuksissa sakkojen määrä voi olla enintään 1 000 000 euroa, yrityksen ollessa kyseessä 2 % sen liikevaihdosta. Sakon määrään vaikuttavat muun muassa rikkomuksen luonne, vakavuus ja kesto, mahdolliset aiemmat rikkomiset sekä yhteistyön aste valvontaviranomaisen kanssa. Henkilötietojen käsittely ilman riittävää oikeusperustetta, tietosuojavastaan nimittämättä jättäminen, tietoturvaloukkauksen tapahtuessa

ilmoitusvelvollisuuden laiminlyönti tai tietosuojaviranomaisen määräyksien noudattamatta jättäminen ovat esimerkkejä vakavimmista rikkeistä. (COM(2012)11 final, 79 artikla, 2 & 6 alakohdat.)

Seuraamus voidaan jättää määräämättä ja antaa kirjallinen varoitus, jos asetusta rikotaan tahattomasti ensimmäisen kerran, jos kyseessä on henkilötietoja ilman kaupallista intressiä käsittelevä luonnollinen henkilö tai alle 250 työntekijän yritys tai järjestö, joka käsittelee henkilötietoja ainoastaan aputoimintona pääasialliseen toimintaansa. (COM(2012) 11 final, artikla 79, alakohta 3.)

Henkilötietodirektiivin 24 artiklassa sanktioista todetaan, että jäsenvaltioiden on määriteltävä sanktiot direktiivin säännösten rikkomistapauksissa ja muutenkin toteutettava toimenpiteet soveltamisen varmistamiseksi. Henkilötietolain mukaisesti tietosuojavaltuutettu tai tietosuojalautakunta voi määrätä uhkasakon tehosteeksi uhkasakkolain mukaisesti (HeTiL 46 §). Aiempaan lainsäädäntöön verrattuna tietosuoja-asetuksen asettamat seuraamukset ovat paljon kireämmät, sillä asetus velvoittaa valvontaviranomaisen määräämään sakon rikkomustilanteessa. Konkreettisesti määritelty rangaistus luultavasti edesauttaa asetuksen noudattamista.

Henkilötietolain 48 §:ssä säädetään henkilörekisteririkkomuksesta. Esimerkiksi tahallaan tai törkeästä huolimattomuudesta tapahtuneesta henkilötietojen käsittelyn tarkoituksen määrittelyn tai rekisteriselosteen laiminlyönnistä annetaan sakkorangaistus. (HeTiL 48 §.) Henkilörekisteririkoksesta on taas kyse muun muassa silloin, jos henkilötietoja käsitellään vastoin käsittelyn yleisiä edellytyksiä, arkaluonteisia tietoja tai henkilötietojen käsittelyä koskevia erityissäännöksiä tai yritetään estää rekisteröityä käyttämästä tarkastusoikeuttaan loukaten rekisteröidyn yksityisyyden suojaa tai aiheuttaen muuta vahinkoa tai haittaa. Henkilörekisteririkoksesta tuomitaan sakkoon tai enintään yhden vuoden vankeuteen. (Rikoslaki 19.12.1889/39 38:9 §.)

Rekisterinpitäjän ja henkilötietojen käsittelijän vastuu sekä rekisteröidyn oikeus korvauksiin määritellään tietosuoja-asetuksen 77 artiklassa. ”Lainvastaisesta käsittelystä tai minkä tahansa toiminnan yhteensopimattomuudesta tämän asetuksen säännösten kanssa” aiheutuvasta vahingosta henkilöllä on oikeus saada korvaus aiheutuneesta vahingosta rekisterinpitäjältä tai henkilötietojen käsittelijältä. Useamman rekisterinpitäjän tai henkilötietojen käsittelijän osallistuttua käsittelyyn, ovat kaikki yhteisvastuullisesti vastuussa korvauksen koko määrästä.

Vastuusta korvaukseen voidaan vapauttaa osittain tai kokonaan, jos pystytään näyttämään, ettei rekisterinpitäjä tai henkilötietojen käsittelijä ole vastuussa vahingon aiheuttaneesta tapahtumasta. (COM(2012) 11 final, artikla 78).

Henkilötietodirektiivin 23 artikla määrittelee korvausvastuun muuten samoin, mutta vastuu on ainoastaan rekisterinpitäjällä, eikä yhteisvastuullisesta korvausvelvollisuudesta säädetä (Henkilötietodirektiivi 23 artikla). Henkilötietolaki säättää rekisterinpitäjän velvolliseksi taloudellisen ja muun vahingon korvaamiseen, jos vahinko on aiheutunut kyseisen lain vastaisesta henkilötietojen käsittelystä (HeTiL 47 §).

4.3 Rekisteröidyn oikeudet

Tietosuoja-asetus pyrkii luomaan rekisteröidylle paremman luottamuksen rekisterinpitäjiin tuomalla henkilötietojen käsittelyä läpinäkyväksi ja tietoa käsittelystä paremmin saataville. Rekisteröidyn oikeus vaatia häntä koskevia tietoja poistettavaksi laajenee, ja rekisteröidylle annetaan oikeus tulla unohdetuksi, eli pyytää kaikkien tietojen poistamista. Asetus myös luo oikeuden vastustaa profilointia ja laajentaa oikeutta vastustaa tietojen käsittelyä.

4.3.1 Läpinäkyvyys ja tiedonsaantioikeus

Tietosuoja-asetuksen 11 artikla luo uuden velvoitteen, jonka mukaan rekisterinpitäjän toimintatapojen täytyy olla läpinäkyvät ja helposti saatavilla olevat, ja kaikki henkilötietojen käsittelyä koskevat tiedot on toimitettava rekisteröidylle helposti ymmärrettävässä muodossa ja selkeällä ja yksinkertaisella kielellä. (COM(2012)11 final, 11 artikla.) Läpinäkyvyyden käsitettä ei tunneta aiemmassa lainsäädännössä.

Rekisterinpitäjän täytyy tietosuoja-asetuksen 14 artiklan mukaisesti toimittaa rekisteröidylle henkilötietoja kerätessä ainakin tiedot rekisterinpitäjän ja tämän edustajan sekä tietosuojavastaavan henkilöllisyydestä yhteystietoineen, henkilötietojen käsittelyn tarkoituksesta ja henkilötietojen säilytysajasta. Lisäksi rekisteröidylle täytyy ilmoittaa tämän oikeudesta pyytää itseään koskevia henkilötietoja rekisterinpitäjältä sekä oikeudesta oikaista, poistaa tai vastustaa kyseisten tietojen käsittelyä. Rekisteröidyn on myös tiedotettava valitusoikeudesta valvontaviranomaiselle yhteystietoineen, henkilötietojen vastaanottajasta tai

vastaanottajaryhmistä, tieto siirretäänkö tietoja kolmanteen maahan tai kansainväliselle järjestölle, sekä muista tiedoista, jotka ovat tarpeen rekisteröidyn kannalta asianmukaisen tietojenkäsittelyn takaamiseksi. (COM(2012)11 final, 14 artikla, 1. kohta.)

Jos tiedot kerätään rekisteröidyltä, rekisteröidylle on ilmoitettava myös, onko henkilötietojen antaminen pakollista vai vapaaehtoista sekä mahdolliset seuraukset, jos tietoja ei anna. Jos henkilötiedot kerätään muulta kuin rekisteröidyltä, täytyy tälle ilmoittaa, mistä ne saatu. Tiedot on toimitettava henkilötietoja tallentaessa tai kohtuullisen ajan kuluttua keräämisestä. (COM(2012)11 final, 14 artikla, 2-3 kohdat.) Tietojen toimittamisesta voidaan poiketa, jos rekisteröity on jo aiemmin saanut tiedot tai henkilötietoja kerättyä muulta kuin rekisteröidyltä tietojen toimittaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa, tai henkilötietojen tallentamisesta säädetään laissa, tai kyseisten tietojen toimittaminen vaikuttaisi muille kuuluviin oikeuksiin ja vapauksiin esimerkiksi yleisen turvallisuuteen tai rikosten selvittämiseen. (COM(2012)11 final, 14 artikla, 5. kohta.)

Henkilötietolain 24 §:än ja Henkilötietodirektiivin 10 artiklaan verrattuna tietosuoja-asetuksen 14 artikla lisää velvollisuuden ilmoittaa tietojen säilytysajasta ja lähteestä, sekä oikeudesta pyytää, oikaista ja poistaa tietoja ja vastustaa tietojenkäsittelyä ja valitusoikeudesta valvontaviranomaiselle. Tietosuoja-asetus laajentaa ilmoitusvelvollisuuden koskemaan sitä, mihin tarkoitukseen ja millä perusteella henkilötietoja käsitellään. Tällä tarkoitetaan sitä, perustuuko tietojenkäsittely rekisteröidyn antamaan suostumukseen, sopimuksen täytäntöönpanoon vai rekisterinpitäjän oikeutettuun etuun. (COM(2012)11 final, 14 artikla, 1. kohta & Henkilötietodirektiivi 10 artikla.)

4.3.2 Tietojen oikaiseminen, poistaminen ja oikeus tulla unohdetuksi

Asetuksen 16 artikla antaa rekisteröidylle oikeuden vaatia virheellisten henkilötietojen oikaisua ja puutteellisten tietojen täydentämistä (COM(2012)11 final, 53). Henkilötietodirektiivin 12 b artiklan mukaan tällainen tietojen oikaisu- tai poisto-oikeus on tapauskohtaista, ja edellyttää tietojen käsittelyn olevan direktiivin vastaista "erityisesti tietojen puutteellisen tai virheellisen luonteen vuoksi" (Henkilötietodirektiivi 12 b artikla).

Uutena oikeutena tietosuoja-asetus tuo oikeuden tietojen poistamiseen ja tulla unohdetuksi. Asetuksen 17 artikla antaa rekisteröidylle oikeuden vaatia henkilötietojensa poistamista, jos tietoja ei tarvita sitä tarkoitusta varten, mihin ne kerättiin tai missä niitä käsiteltiin, rekisteröity peruuttaa suostumuksensa tietojen käsittelyyn tai vastustaa tietojensa käsittelyä tai tietojen käsittely mistä tahansa syystä ei ole tietosuoja-asetuksen mukaista.

Tietojen poistamisen vaatiminen myös kieltää tietojen edelleen luovuttamisen. Asetuksessa mainitaan, että etenkin rekisteröidyn alaikäisenä antamat tiedot on mahdollista vaatia poistettavaksi. Henkilötietodirektiivi mainitsee 12 b artiklassa oikeuden tietojen poistamiseen, mutta asetus täsmentää tätä oikeutta. Rekisterinpitäjän täytyy ilmoittaa kolmansille osapuolille rekisteröidyn pyynnöstä poistaa henkilötietojen kopiot, jäljennökset sekä niihin liittyvät linkit. (COM(2012)11 final, 9 artikla & Henkilötietodirektiivi 12 artikla b-kohta.)

Oikeutta tulla unohdetuksi on käsitelty mediassa runsaasti Euroopan unionin tuomioistuimen niin sanotun "Google-päätöksen" jälkeen. Kyse vuonna 1998 julkaistuista lehtiartikkeleista, jotka käsittelivät espanjalaisen miehen taloudellisia ongelmia. Miehen nimeä hakiessa Internetistä Googlen hakukone antoi linkin kyseisiin artikkeleihin. Mies halusi tiedot poistettavaksi, sillä tiedot olivat vanhentuneita ja artikkelissa mainitut velkaongelmat loppuun käsiteltyjä. Tuomioistuin määräsi päätöksessään Googlen poistamaan artikkeliin viittaavat linkit. Tuomioistuin perusteli päätöstään sillä, että Google käsittelee henkilötietoja tavalla, jolla sitä tulee pitää rekisterinpitäjänä, ja liikkeen tytäryhtiö toimii EU-maan alueella, jolloin yhtiön täytyy henkilötietodirektiivin toimipaikka-säädöksen nojalla noudattaa kyseistä direktiiviä. Tuomioistuin katsoi, että alun perin laillinen käsittely voi muuttua direktiivin vastaiseksi, jos tiedot eivät enää ole asianmukaisia, olennaisia tai ne ovat liian laajoja. Tuomioistuin tulkitsi henkilötietodirektiiviä niin, että Google on velvollinen poistamaan linkit hakutuloksista. (Euroopan unionin tuomioistuin 2014, viitattu 7.5.2015.)

4.3.3 Oikeus vastustaa henkilötietojen käsittelyä ja profilointia

Asetuksen 19 artiklan mukaan rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä, jos se perustuu rekisteröidyn elintärkeiden etujen suojaamiseksi, yleistä etua koskevan tehtävän suorittamiseen, rekisterinpitäjän julkisen vallan käyttöön tai rekisterinpitäjän oikeutetun edun toteuttamiseksi, jos tämä etu ei syrjäytä rekisteröidyn etuja, perusoikeuksia tai -vapauksia.

Suoramarkkinointia varten tapahtuvaa käsittelyä on oikeus vastustaa maksutta, ja rekisteröidylle on tarjottava tätä oikeutta nimenomaisesti, erillään muusta tiedotuksesta. (COM(2012)11 final, 19 artikla.)

Henkilötietodirektiivi antaa rekisteröidylle oikeuden vastustaa henkilötietojensa käsittelyä sen perustuessa yleistä etua koskevan tehtävän suorittamiseen, rekisterinpitäjän tai tiedot saavan sivullisen julkisen vallan käyttämiseen taikka jos käsittely on oikeutettua rekisterinpitäjän tai tiedot saavan sivullisen intressin toteuttamiseksi, kunhan tämä ei syrjäytä rekisteröidyn perusoikeuksia ja -vapauksia. Suoramarkkinointia koskevaa erillismainintaa ei direktiivissä ole. (Henkilötietodirektiivi 14 artikla.)

Uutena oikeutena asetus tuo oikeuden vastustaa profilointia. 20 artiklan mukaan luonnollisella henkilöllä on oikeus olla joutumatta kohteeksi toimenpiteessä, joka tuo hänelle oikeusvaikutuksia tai muuten vaikuttaa häneen merkittävällä tavalla, ja joka on tehty ainoastaan automaattisen tietojenkäsittelyn perusteella esimerkiksi taloudellisen tilanteen, terveyden, henkilökohtaisten mieltymysten tai käyttäytymisen ennakkointia tai analysoimista varten. Profilointia voidaan suorittaa, vain jos se perustuu sopimuksen tekemisen tai täytäntöönpanon yhteydessä taikka rekisteröidyn suostumukseen, se on hyväksytty unionin tai jäsenvaltion lainsäädännössä. (COM(2012)11 final, 20 artikla.)

4.3.4 Oikeussuojakeinot

Tietosuoja-asetuksen 73 artiklassa rekisteröidylle määritellään oikeus tehdä valitus valvontaviranomaiselle, jos asetuksen säännöksiä ei ole hänen henkilötietojensa käsittelyssä mielestään noudatettu. Valituksen voi tehdä minkä tahansa jäsenvaltion valvontaviranomaiselle. Myös mikä tahansa rekisteröityjen henkilötietojen suojaan liittyviä oikeuksia suojelemaan asianmukaisesti perustettu elin tai yhdistys voi tehdä valituksen yhden tai useamman rekisteröidyn puolesta. (COM(2012)11 final, 73 artikla.) Sama oikeus esitetään henkilötietodirektiivissä (Henkilötietodirektiivi 28 artikla 4 kohta)

Jos valvontaviranomaisen päätökseen ollaan tyytymättömiä, niin luonnollinen kuin oikeushenkilö ovat oikeutettuja oikeussuojakeinoihin, eli valittamaan tuomioistuimeen. Valitus täytyy tehdä sen jäsenvaltion tuomioistuimeen, jonka valvontaviranomaisen päätöksestä halutaan valittaa. Jos

rekisteröityä koskevan päätöksen on tehnyt toisen jäsenvaltion valvontaviranomainen, hänen on mahdollista pyytää asuinvaltionsa valvontaviranomainen aloittamaan oikeudelliset menettelyt päätöksen tehnyttä valvontaviranomaista vastaan. (COM(2012)11 final, 74 artikla.) Myös tietosuojadirektiivin mukaan valvontaviranomaisen päätöksestä voi valittaa tuomioistuimeen (Henkilötietodirektiivi 28 artikla 3 kohta).

Rekisteröity luonnollinen henkilö voi nostaa kanteen tuomioistuimessa rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, jos hänen mielestään henkilötietojen käsittelyssä ei ole noudatettu tietosuoja-asetusta ja hänen oikeuksiaan on näin loukattu. Kanne on nostettava joko rekisterinpitäjän taikka henkilötietojen käsittelijän toimipaikkavaltion tuomioistuimessa tai rekisteröidyn vakinaisen asuinpaikan tuomioistuimessa. Jos rekisterinpitäjä on viranomainen jonka toiminta liittyy julkisen vallan käyttöön, kanne täytyy nostaa siinä jäsenvaltiossa, jonka viranomainen on kyseessä. (COM(2012)11 final, 75 artikla.) Tietosuojadirektiivi mahdollistaa myös kanteentekomahdollisuuden, jos henkilötietojen käsittelyn yhteydessä oikeuksia loukataan (Henkilötietodirektiivi 22 artikla).

5 VAIKUTUKSET OULUN AMMATTIKORKEAKOULUSSA

Työtä varten haastateltiin Oamkin vararehtori Jyrki Laitista, tietohallinnon päällikköä Samuli Malista ja tietohallinnossa sovellussuunnittelijana työskentelevää Anna-Liisa Mattilaa. Haastattelut olivat vapaamuotoisia teemahaastatteluja ja pohjautuivat haastateltaville ennalta lähetettyihin kysymyksiin. Haastattelujen tarkoituksena on selvittää miten tietosuoja huomioidaan ja ollaanko asetuksesta tietoisia, sekä onko uudistukseen jo ryhdytty varautumaan.

Jyrki Laitinen kertoo käsittelevänsä tietosuoja-asioita pääasiassa alaisuudessaan toimivien IT- ja tietohallinto-osastojen kautta. Laitinen on toiminut aiemmin yksikönjohtajana, jolloin hän tutustui tietosuojaan ja henkilökisterijärjestelmään myös rekistereiden käyttäjänä. (Laitinen 28.5.2015, haastattelu.) Samuli Malinen huolehtii tietohallinto-osaston osalta tietosuoja-asioista (Malinen 3.6.2015, haastattelu). Anna-Liisa Mattilalle tietosuoja näkyy verkko-opetukseen liittyvien työtehtävien kautta (Mattila 5.6.2015, haastattelu).

5.1 Tietosuoja ja sen uudistuminen Oamkissa

Haastatellut kokivat nykyisen tietosuojalainsäädännön riittävän kattavaksi, ja Suomen tilanteen olevan hyvä. Sääntely on monipuolista, eikä sen noudattamisessa ole ongelmia ollut. Laitinen kokee nykyisen lain sekavana hallinnolliselta kannalta, ja pitääkin tervetulleena selkeytystä ja yhteneväisiä ohjeistuksia. Myös muut haastateltavat ovat samaa mieltä; kaikille yhteisiä pelisääntöjä EU:n sisällä pidetään hyvänä ratkaisuna. (Laitinen 28.5.2015, haastattelu; Malinen 3.6.2015, haastattelu & Mattila 5.6.2015, haastattelu.)

Oamkin tärkeimpiin henkilökistereihin kuuluvat opiskelija- ja henkilöstökisterit. Tämän hetkinen henkilökisterijärjestelmä on vanhan yksikköjärjestelmän mukainen, ja se sisältää myös niin sanottuja epävirallisia rekistereitä. (Laitinen 28.5.2015, haastattelu.) Myös Mattila epäilee, ettei kaikista rekistereistä olla tietoisia ja nostaa esille sosiaali- ja terveysalan yksikössä opiskelijoiden tarjoamia palvelut, ja pohtii, miten niiden yhteydessä asiakkailta kerätyt tiedot säilytetään. (Mattila 5.6.2015, haastattelu.)

Haastatteluissa nousi esiin henkilöstön tietosuojaaosaaminen. Oamk ei tarjoa työntekijöilleen erityisiä tietosuojakoulutuksia, vaan tiettyyn tehtävään liittyvät tietosuoja-asiat käydään tarvittaessa läpi. Tietohallinnon mukaan tietosuojakoulutuksille on kuitenkin tarvetta. Malinen toteaa, että tietosuojakoulutus ja -tietoisuus sekä muistuttaminen oikeista toimintatavoista ovat yksi tärkeimmistä tulevan tietosuojavastaavan tehtävistä (Malinen 3.6.2015, haastattelu). Mattila toivoo, että Oamkin prosesseista vastaavat henkilöt ja tietosuojavastaava kävisivät työskentelyprosessit läpi, varmistaen, että tietosuojakäytänteitä noudatetaan koko prosessin ajan (Mattila 5.6.2015, haastattelu).

Tietosuoja-asetuksen lopullista voimaantuloa edeltävää kahden vuoden siirtymäaika pidetään riittävänä uudistusten toteuttamiselle, ja ammattikorkeakoulujen rehtorineuvosto, jossa yhteiset käytänteet sovitaan, aloittaa neuvottelut todennäköisesti jo tulevan syksyn aikana (Laitinen 28.5.2015, haastattelu). Parhaillaan käynnissä oleva organisaatiouudistus vaikuttaa jonkin verran tietosuojaan, sillä vanhat tietojärjestelmät uudistetaan myös. Rekistereiden varsinaisen sisältöön Malinen ei arvele organisaatiomuutoksen vaikuttavan, mutta asia jää tietosuojavastaavan hoidettavaksi (Malinen 3.6.2015, haastattelu).

Laitinen ja Malinen pitävät Oamkin vahvuuksina hyvää teknistä valmiutta, jo olemassa olevia järjestelmiä ja hyviä tietoturvakäytänteitä. Pääsääntöisesti henkilörekisterit ja rekisteriselosteet ovat ajan tasalla ja ainakin tietohallinnossa uudistuksesta ollaan tietoisia ja siihen liittyviä muutoksia on jo ryhdytty selvittämään. (Laitinen 28.5.2015, haastattelu & Malinen 3.6.2015, haastattelu.) Sopivan henkilön löytäminen tietosuojavastaavaksi ja tämän toimenkuvan päättäminen voi olla haastavaa. Haasteena pidetään myös koko rekisterijärjestelmän selvittämistä ja selkeyttämistä sekä tietosuojatietoisuuden parantamista koko henkilökunnan keskuudessa. (Laitinen 28.5.2015, haastattelu; Malinen 3.6.2015, haastattelu & Mattila 5.6.2015, haastattelu.)

5.2 Tietosuojavastaava

Tietosuojavastaavan palkkaaminen ei Laitisen mukaan ole taloudellinen tai hallinnollinen haaste Oamkille. Hän toteaa, että tietosuojasta vastaavan henkilön toimenkuvan suunnittelu on hankalampaa kuin itse palkkaus; ei ole vielä varmaa onko toimi koko- vai osapäiväinen. (Laitinen 28.5.2015, haastattelu.) Malisen mukaan osapäiväinen toimi riittäisi, sillä muutenkin hallinnossa

pyritään niukkuuteen. Oamkin ollessa osa Oulun seudun koulutuskuntayhtymää sillä oli yksi tietosuojavastaava, joten noin 50 %:n työaika voi nykytilanteessa olla riittävä. (Malinen 3.6.2015, haastattelu.)

Tietosuoja-asiat on Oamkissa vastuutettu usealle eri taholle, opiskelijarekisteri kuuluu tietohallinnon ja opiskelijapalveluiden vastuualueeseen, henkilöstöasiat henkilöstöhallinnolle ja osin Monetra Oy:lle, joka hoitaa muun muassa Oamkin palkanlaskennan ja matkalaskut. Lisäksi Oamkissa toimii tila- ja turvallisuusvastaava, joka vastaa fyysisestä turvallisuudesta. Tilanteissa, joissa vastuuhenkilöä ei ole erikseen nimetty, vastuu on rehtorilla. Henkilö, jonka kanssa keskustella ja kehittää tietosuojaa, on tarpeellinen, sillä tämä on luultavasti helpommin tavoitettavissa kuin koulun johto. (Laitinen 28.5.2015, haastattelu.)

Malinen korostaa, että vastuuta on jaettu usealle tasolle, eikä vielä ole selvä mitä kaikkea tulevan tietosuojavastaavan toimenkuvaan kuuluu. Vastuun siirtäminen yhdelle henkilölle voi toisaalta selkeyttää, mutta myös vaikeuttaa toimintaa. Asioiden keskittäminen yhdelle henkilölle helpottaa kokonaiskuvan hahmotusta, mutta tietosuojan kenttä voi olla turhan laaja yhden henkilön hoidettavaksi. Tavoitettavuus koettiin myös ongelmaksi, tehtävät täytyisi hoitaa ajallaan myös tietosuojavastaavan poissa ollessa. Tietosuojavastaavan toimenkuvasta sovitaan luultavasti syksyn aikana. (Malinen 3.6.2015, haastattelu.)

5.3 Rekisteröidyn asema

Uudessa asetuksessa rekisteröidylle annettava oikeus tulla unohdetuksi koetaan ristiriitaiseksi. Tällä hetkellä opiskelijoiden käyttäjätunnukset poistuvat automaattisesti valmistumisen jälkeen, mutta asetuksen myötä myös muita tietoja voidaan pyytää poistettavaksi koulun rekistereistä. Malisen mukaan oikeus tulla unohdetuksi on tietosuojan lisäksi myös oikeusturvakysymys, sillä koulun täytyy tarvittaessa pystyä toimittamaan todistuskopiot tuhoutuneiden tilalle. Lisäksi koulu on velvollinen toimittamaan tietoja esimerkiksi opintosuorituksista ja valmistuneista eri viranomaisille. Malinen toteaa, että heidän täytyy varmistaa viranomaisilta se, mistä järjestelmistä ja millä laajuudella tietojen poistaminen voidaan tehdä. (Malinen 3.6.2015, haastattelu.) Myös Mattilan mukaan tietojen poistaminen kaikista rekistereistä ei ole mahdollista, ja tällaiseen poikkeustilanteeseen täytyy varautua selvittämällä etukäteen tarvittavat toimenpiteet. Hän esittää

kysymyksen, tarkoittaisiko poistaminen Oamkin rekistereistä koulun näkökulmasta sitä, ettei opiskelija olisi enää valmistunut Oamkista. (Mattila 5.6.2015, haastattelu.)

Haastatteluissa kävi ilmi, että vaikka rekisteriselosteet ovat julkisesti esillä, ne saattavat olla puutteellisia tai vaikeasti löydettävissä. Rekisteriselosteista ei myöskään ole englanninkielistä versiota kansainvälisille opiskelijoille. Malisen mukaan rekisteriselosteita tulisi tarkastella säännöllisemmin, ja Mattila ehdottaa, että linkit rekisteriselosteisiin lisätään jokaisen järjestelmän kirjautumissivulle (Malinen 3.6.2015, haastattelu & Mattila 5.6.2015, haastattelu).

Vaikkei tapa, miten tiedot siirtyvät järjestelmästä toiseen automaattisesti esimerkiksi opiskelupaikkahakujärjestelmästä koululle, ole lainsäädännön vastainen, olisi hyvä kertoa selkeästi opiskelijalle mitä kautta tiedot on saatu. Uuden asetuksen mukanaan tuomat tilivelvollisuus ja läpinäkyvyys toivottavasti parantavat tilannetta ja lisäävät avoimuutta rekisteröidyn ja rekisterinpitäjän välillä.

Oamkin valmiudet tietosuoja-asetuksen tuloon ovat hyvät. Ohjelmistot ja käytänteet ovat tietohallinnossa kunnossa, ja neuvottelut muun muassa tietosuojavastaavasta käynnistyvät jo syksyn 2015 aikana. Tietosuojaosaaminen ei kuitenkaan ole niin hyvällä tasolla kuin voisi olla, sillä koulutuksia tietosuojasta ei järjestetä, vaan tietosuoja-asiat käsitellään työtehtäviin perehdytyksen yhteydessä. Näkyvin muutos Oamkissa on tietosuojavastaava, jonka uskotaan selkeyttävän vastuunjako ja joka päivittää henkilörekisterijärjestelmän uuden asetuksen ja uuden organisaation mukaiseksi. Henkilörekistereissä tapahtuvat muutokset eivät näy ulospäin, mutta ne vaikuttavat positiivisesti rekisteröityjen tietosuojaan.

6 JOHTOPÄÄTÖKSET

Tietosuojaan tärkeys korostuu Internetin ollessa osa arkipäivää ja tietotekniikan ollessa käytössä kaikkialla ympärillämme. Huoli omien tietojen turvasta on aiheellinen, sillä tietoturvaohjeita kohdistuu niin suuriin kuin pieniin organisaatioihin. Vaikka Suomen lainsäädäntö suojaakin yksityisyyttä tällä hetkellä melko hyvin, voi olla, että henkilötietoja käsittelevä taho noudattaa jonkin toisen valtion ohjeistusta, jolloin tietosuoja ei ole niin hyvä. EU:n alueella toimivat rekisterinpitäjät ovat yhtenäisen ohjeistuksen tarpeessa tiedon siirtyessä valtioiden rajojen yli ja tietotekniikan tavoittaessa yhä suuremman osan alueen väestöstä.

Opinnäytetyön tavoitteena oli selvittää miten Euroopan tietosuoja-asetus vaikuttaa henkilötietojen suojaan ja minkälaisia käytännön vaikutuksia sillä on Oulun ammattikorkeakoulu Oy:n toimintaan. Opinnäytetyöllä pyritään vastaamaan kysymyksiin

- Millaisia muutoksia EU:n uusi yleinen tietosuoja-asetus tuo lainsäädäntöön?
- Miten Oamk Oy:n tulee varautua toiminnassaan tietosuoja-asetuksen velvoitteisiin?
- Miten tietosuoja-asetus vaikuttaa rekisteröidyn asemaan Oamk Oy:ssä?

Suurin tietosuoja-asetuksen tuomista muutoksista on lainsäädännön yhtenäistäminen Euroopan unionin jäsenvaltioiden välillä. Aiempaan direktiivimuotoiseen säädöksen verrattuna tämä luo kaikkien jäsenvaltioiden kansalaisille yhdenmukaiset oikeudet ja helpottaa yritysten toimimista jäsenvaltioiden rajojen yli. Asetus luo rekisterinpitäjälle tiukempia vaatimuksia henkilötietojen käsittelyyn esimerkiksi suostumuksen saannissa ja henkilötiedoille tehtyjen toimenpiteiden todentamisessa. Tietosuoja muuttuu oletusarvoksi ja se on sisäänrakennettu ohjelmiin, eli vastuu asetuksen myötä siirtyy yhä enemmän rekisterinpitäjälle. Vastuu ulotetaan myös henkilötietojen käsittelijälle. Sanktiouhkalla halutaan edistää yhteisten sääntöjen noudattamista.

Oulun ammattikorkeakoulussa tietosuojaan uudistuminen on jo huomioitu ja alustavia keskusteluita aiheesta on jo käyty, vaikkei lopullisia päätöksiä ole vielä tehty. Kokonaisuutena tietosuoja on hyvällä tasolla, mutta puutteitakin on. Oamkin vahvuuksia ovat jo hyvät tekniset valmiudet muutoksiin sekä toimiva tietoturva. Haasteeksi Oamkissa nousee kokonais kuvan hahmottaminen, tietosuojavastaavan toimenkuvan selvittäminen ja koko henkilöstön osaamisen huomioiminen tietosuoja-asioissa.

Tietosuojavastaavan asettaminen on näkyvin muutos Oamkissa, sillä todennäköisesti vastuu tietosuoja-asioista keskitetään tähän työtehtävään. Tietosuojavastaava tulee tekemään tiivistä yhteistyötä niin hallinnon, tietohallinnon, IT-osaston kuin muidenkin tahojen kanssa. Tällä hetkellä ongelmia aiheuttaa selkeän vastuutahon puuttuminen, sillä tämänhetkisenä vastuuhenkilönä toimivaa rehtoria on vaikea tavoittaa. Henkilörekisterijärjestelmän selkeyttäminen, rekisteriselosteiden laadinta ja päivittäminen asetuksen vaatimusten mukaisiksi sekä henkilöstön tietosuojaosaamisen parantaminen ovat myös tarvittavia muutoksia. Sekava rekisterijärjestelmä, joka on pysynyt usean organisaatiouudistuksen ajan muuttumattomana, voi pitää sisällään yllätyksiä, joihin tietosuojavastaavan on puututtava. Voi olla, että tietojärjestelmät sisältöineen muuttuvat, vanhentuneet ja tarpeettomat rekisterit poistetaan ja uusia rekistereitä syntyy.

Opiskelijalle koko tämänhetkinen rekisterijärjestelmä on melko huomaamaton, sillä vaikka rekisteriselosteet ovat saatavilla, ne ovat hankalasti esillä, ja kansainvälisillä opiskelijoilla ei ole mahdollisuutta tutustua niihin. Rekisteröidylle tietosuojauudistus tuo rekisteriselosteet paremmin saataville. Oikeutta tulla unohdetuksi ei luultavasti voida Oamkissa käyttää sen asetuksessa määritellyllä laajuudella johtuen koulun velvollisuudesta säilyttää tiettyjä asiakirjoja vielä opiskelijan valmistumisen jälkeenkin.

Kahden vuoden siirtymäajan puitteissa Oamk pystyy toteuttamaan vaaditut muutokset, eikä suuria haasteita uudistuksessa pitäisi tulla. Asetukseen valmistautuminen kannattaa aloittaa kuitenkin heti, jotta tarvittavat toimenpiteet ehditään pohtia huolellisesti. Tärkeimpänä toimenpiteenä on asianmukaisen koulutuksen ja osaamisen omaavan henkilön nimeäminen tietosuojavastaavaksi. Tämän jälkeen voidaan ryhtyä selvittämään muita organisaatiossa tarvittavia muutoksia.

7 POHDINTA

Euroopan Unionin massiivinen lainsäädäntöhanke tietosuojan yhtenäistämiseksi on herättänyt keskustelua puolesta ja vastaan, ja viimein se on valmistumassa tämän vuoden lopulla. Asetusta on moitittu liian laajaksi ja tehottomaksi, mutta se on myös herättänyt ihmisten kiinnostuksen tietosuojaan, mikä on ainoastaan hyvä asia. Huoli omasta yksityisyydestä toimii yksilön näkökulmasta kenties tehokkaampana tietosuojakeinona kuin valtavan velvoitemäärän asettaminen rekisterinpitäjätaholle, mutta kuten tietosuoja-asetuksen perusteluissa mainitaan, vastuu tietosuojasta täytyy olla rekisterinpitäjällä, eikä sitä voi jättää vain rekisteröidyn itse huolehdittavaksi.

Kyberturvallisuus on noussut vasta parin viime vuoden aikana yhdeksi suurimmista riskeistä yritystoiminnassa, ja tämä voi aiheuttaa monille yrityksille ongelmia tietosuoja-asetuksen kahden vuoden siirtymäaika jäädessä lyhyeksi. Suurin uhka yritysten kannalta on, ettei uhkia ymmärretä vaikka ne huomioitaisiin. (Lehtinen 2015, viitattu 16.4.2015.) Tietosuoja-asetusta on moitittu raskaaksi pienten yritysten kohdalla, sillä niissä tietosuojaa ei aiemmin ole huomioitu ainakaan asetuksen velvoittamalla laajuudella. Asetusta on muokattu alkuperäisestä komission ehdotuksesta kevyempään suuntaan, mikä herättää kysymyksen: vesittyvätkö sen tavoitteet velvoitteiden jousaessa?

Tämän työn tavoitteena oli selvittää millaisia muutoksia tietosuoja-asetus tuo lainsäädäntöön ja miten nämä muutokset Oulun ammattikorkeakoulun toimintaan. Työ toteutettiin lainopillisena tutkimuksena ja lisäksi haastatteleamalla Oamkin työntekijöitä pyrittiin selvittämään tietosuojan nykytilannetta ja varautumista uudistukseen. Työn tuloksina selvisi, että suurimmat muutokset lainsäädännössä liittyvät rekisterinpitäjälle tuleviin velvollisuuksiin ja sanktiouhkaan sekä rekisteröidyn oikeuksien laajentamiseen. Oamkin toimintaan asetus vaikuttaa näkyvimmin velvoittamalla nimeämään tietosuojavastaavan.

Työssä onnistui laajan teoriapohjan koostaminen selkeäksi kokonaisuudeksi. Koen onnistuneeni löytämään ajankohtaista ja monipuolista lähdeaineistoa. Työtä tehdessä löysin jatkuvasti lisää lähteitä, varsinkin englanninkielistä materiaalia olisi ollut tutkittavana tuhansia sivuja, lisäksi aiheesta on paljon kirjallisuutta. Onnistuin mielestäni löytämään työni ja aiheeni kannalta oleelliset ja ajantasaisimmat lähteet.

Työtä olisi voinut parantaa syventymällä enemmän haastatteluihin. Nyt työ on pitkälti teoriapohjainen ja käytännön osuus jää kapeaksi. Haastatteluista henkilöistä kaikkien työtehtävissä näkyi tietosuoja jollain tasolla, ja tämä saattaa antaa väärentyneen kuvan Oamkin organisaation tietosuojasta. Koko organisaation tilanne olisi kenties tullut selvemmin esille, jos haastateltavina olisi ollut työntekijöitä, joille tietosuoja ei ole jokapäiväinen asia ja työssä olisi vertailtu eri osastoja laajemmin. Tehdyistä haastatteluista kävi ilmi kuitenkin useita puutteita tietosuojan tasossa, joten lisähaastattelut eivät välttämättä olisi tuoneet paljoa lisäarvoa työlle.

Haastatteluissa olisi lisäksi ollut hyvä keskittyä vahvemmin tietosuoja-asetuksen tuomiin uudistuksiin, jolloin olisi syntynyt konkreettisempia muutosehdotuksia Oamkin organisaation toimintaan. Nyt nämä ajatukset jäivät melko yleiselle tasolle, joten työn validiteetti jää vajaaksi. Myös haastattelujen toteuttaminen yhtenä ryhmähaastatteluna olisi voinut herättää esiin aiheita, joista en huomannut kysyä. Koen kuitenkin löytäneeni haastatteluista oleelliset asiat. Työn tuloksia voidaan kuitenkin pitää melko luotettavina, sillä käytetty lähdemateriaali on ajankohtaista.

Opinnäytetyön tekeminen oli haastava prosessi, sillä en aiemmin ole kirjoittanut vastaavia laajoja tekstejä. Erityisesti haastatteluosio tuotti ongelmia, sillä aiempaa kokemusta haastattelemisesta ei ollut. Oikeiden kysymysten valinta ja muotoilu riittävän aineiston saamiseksi mietitytti. Itsenäisesti työskentely oli haastavaa, sillä en asettanut itselleni minkäänlaisia takarajoja, joten työn valmistuminen venyi naurettavan pitkäksi. Jos olisin tehnyt itselleni aikataulun ja noudattanut sitä, työ olisi valmistunut jo keväällä. Itsenäinen kirjoittaminen aina aiheenvalinnasta raportin sisällön hiomiseen oli haastavaa, mutta palkitsevaa. Tietyn aikarajan saatuaani pystyin motivoimaan itseäni tehokkaaseen työskentelyyn. Prosessin aikana opin tiedonhakua, tietojen tarpeellisuuden arviointia sekä ammatillista kirjoittamista.

Jatkotutkimusaiheena voisi muutaman vuoden kuluttua selvittää, miten Oulun ammattikorkeakoulu Oy on onnistunut toteuttamaan asetuksen vaatimukset. Asetuksen vaikutusten tutkiminen ja vertailu kahdessa erityyillisessä organisaatiossa voisi olla mielenkiintoinen aihe.

LÄHTEET

Ammattikorkeakoululaki 932/2014.

Eduskunta 2015. U 21/2012 vp, U-jatkokirje 26.02.2015. Komission ehdotus asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus). Viitattu 12.3.2015,

<http://217.71.145.20/TRIPviewer/show.asp?tunniste=U+21/2012+4.+OM+26.02.2015&base=euyk&irj&palvelin=www.eduskunta.fi&f=WORD>.

Euroopan ihmisoikeussopimus. 2015. Viitattu 1.12.2014, http://www.echr.coe.int/Documents/Convention_FIN.pdf.

Euroopan parlamentin ja neuvoston asetukset yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) COM(2012) 11 final. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FI:PDF>.

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (Henkilötietodirektiivi). Viitattu 8.4.2015, <http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:31995L0046&from=fi>.

Euroopan unionin neuvosto. 2015a. Oikeus- ja sisäasioiden neuvosto, 12.-13.03.2015. Viitattu 24.3.2015, <http://www.consilium.europa.eu/fi/meetings/jha/2015/03/12-13/>.

Euroopan unionin neuvosto. 2015b. Yleinen tietosuoja-asetus. Viitattu 12.3.2015, <http://www.consilium.europa.eu/fi/policies/data-protection-reform/data-protection-regulation/>.

Euroopan unionin perusoikeuskirja 2015. Viitattu 15.4.2015, http://www.europarl.europa.eu/charter/pdf/text_fi.pdf.

Euroopan unionin tuomioistuin. 2014. Lehdistötiedote nro 70/14. Viitattu 7.5.2015, <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fi.pdf>.

Eurooppa-neuvosto. 2010. Tukholman ohjelma 2010/C 115/01. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:fi:PDF>.

Eurooppatiedotus. 2015. Lissabonin sopimus. Viitattu 24.3.2015, <http://www.eurooppatiedotus.fi/public/default.aspx?contentid=191396&contentlan=1#.VRE-ivmsVqU>.

European Commission. 2015a. Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market. Viitattu 16.4.2015, http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

European Commission. 2015b. SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union. Viitattu 20.4.2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

European Commission. 2015c. Progress on EU data protection reform now irreversible following European Parliament vote. Viitattu 22.4.2015, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

European Commission. 2015d. Tietosuoja: neuvosto yleisnäkemykseen. Viitattu 31.8.2015, <http://www.consilium.europa.eu/fi/press/press-releases/2015/06/15-jha-data-protection/>.

HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

Henkilötietolaki 22.4.1999/523.

Komission asetus N:o 611/2013. 2013. Viitattu 24.4.2015, http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2013.173.01.0002.01.FIN.

Korhonen, R. 2003. Perusrekisterit ja tietosuoja. Helsinki: Edita Prima Oy.

Laitinen, J., vararehtori, Oulun ammattikorkeakoulu. 2015. Haastattelu 28.5.2015. Tekijän hallussa.

Lehtinen, P. 2015. Kilpailuetua kyberturvallisuudesta ja tietosuojasta. Viitattu 15.4.2015, <http://issuu.com/kpmgfinland/docs/view-1-2015-6.6mt/12>.

Malinen, S., tietohallintopäällikkö, Oulun ammattikorkeakoulu. 2015. Haastattelu 3.6.2015. Tekijän hallussa.

Mattila, A-L., sovellussuunnittelija, Oulun ammattikorkeakoulu. 2015. Haastattelu 5.6.2015. Tekijän hallussa.

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. Helsinki: Lakimiesliiton kustannus.

Oikeusministeriö. 2014. Euroopan unionin tietosuojalainsäädännön uudistaminen. Viitattu 15.12.2014, <http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html>.

Osakeyhtiölaki 21.7.2006/624.

Oulun ammattikorkeakoulu 2015a. Oulun ammattikorkeakoulun esittelykalvot 2014. Viitattu 24.3.2015, <http://www.oamk.fi/utills/opendoc.php?aWRfZG9rdW1lbnR0aT02Mzg1>.

Oulun ammattikorkeakoulu 2015b. Yhteishaku alkaa 17.3. – Oamkissa yli 1 600 aloituspaikkaa. Viitattu 24.3.2015, http://www.oamk.fi/fi/tietoa-oamkista/ajankohtaista/?kieli=&ak_osio=uutisjuttu&kid=25&id=43623.

Oulun ammattikorkeakoulu 2015c. Johtosääntö. Sisäinen lähde. Viitattu 24.4.2015, https://oiva.oamk.fi/tietoa_opiskelusta/opintoihin_vaiuttaminen/johtosaanto/.

Oulun ammattikorkeakoulu 2015d. Tasekirja. Sisäinen lähde. Viitattu 8.5.2015, https://heimo.oamk.fi/ohjeet_ja_oppaat/talous/tiedotteet/.

Oulun ammattikorkeakoulu 2015e. Hallitus pöytäkirja nro 9 8.6.2015. Sisäinen lähde. Viitattu 31.8.2015, https://oiva.oamk.fi/tietoa_opiskelusta/opintoihin_vaiuttaminen/poytakirjat/.

Perustuslaki 11.6.1999/731.

Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Helsinki: Talentum.

Rikoslaki 19.12.1889/39.

Suomen ulkoasiainministeriö. 2015. Ihmisoikeustuomioistuin. Viitattu 8.1.2015, <http://www.finlandcoe.fr/public/default.aspx?nodeid=35770>.

SVT. 2014. Väestön tieto- ja viestintätekniikan käyttö [verkojulkaisu]. Viitattu: 28.4.2015, http://www.stat.fi/til/sutivi/2014/sutivi_2014_2014-11-06_tie_001_fi.html.

Tietosuojatyöryhmä. 2012. Lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista. Viitattu 8.4.2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_fi.pdf.

Tietosuojavaltuutetun toimisto. 2010. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Viitattu 30.3.2015, http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/opaat/6JfqN4sf1/Tietosuojavastaavan_toimenkuva_tehtavat_ja_asema.pdf.

U 21/2012 vp. Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi) Viitattu 26.1.2015, <http://www.eduskunta.fi/valiokuntakasittely/U+21/2012>.

United for Human Rights. 2014. International Human Rights Law. Viitattu 8.1.2015, <http://www.humanrights.com/what-are-human-rights/international-human-rights-law.html>.

United Nations Human Rights. 2015. Universal Declaration of Human Rights. Viitattu 8.1.2015, <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=fin>.

Voutilainen, T. 2012. Oikeus tietoon. Helsinki: Edita.

Internet World Stats. 2015. Internet in Europe Stats. Viitattu 29.4.2015, <http://www.internetworldstats.com/stats9.htm>

LIITTEET

Liite: Opinnäytetyöhaastattelu

EU:N YLEINEN TIETOSUOJA-ASETUS JA SEN VAIKUTUKSET OAMK OY:SSÄ

Haastateltavan tausta

- Nimi
- Asema Oamkissa
- Saako nimen julkaista työssä?

Tietosuojaan nykytilanne

- Millaiseksi koet tämänhetkisen tietosuojalainsäädännön?
- Miten Oamk huolehtii henkilökunnan tietosuojaosaamisesta?
- Millainen vastuunjako Oamkissa on tietosuoja-asioissa?
- Minkä tyyppisiä/ mitä henkilörekistereitä Oamkissa on?

Tietosuoja-asetus ja sen vaikutukset

- Miten hyvin olet tutustunut tietosuoja-asetusehdotukseen?
- Onko asetuksen tuomiin vaatimuksiin varauduttu etukäteen?
- Minkä koet olevan suurin haaste tietosuoja-asetuksen säännösten toteuttamisessa Oamkissa?
- Näkyvätkö muutokset ulospäin/rekisteröidyille?
- Millaisia vaikutuksia asetuksella on työtehtäviisi?
- Millaisia taloudellisia vaikutuksia asetuksella on?
- Onko tulevalla organisaatiouudistuksella vaikutusta tietosuojaan?