Tietosuoja-asetuksen vaatimusten täyttyminen Turun yliopiston henkilörekistereissä

Diplomityö
Turun yliopisto
Tietotekniikan laitos
Tietoliikennetekniikka
2022
Olli Leppänen

TURUN YLIOPISTO
Tietotekniikan laitos

Olli Leppänen: Tietosuoja-asetuksen vaatimusten täyttyminen Turun yliopiston henkilörekistereissä

Diplomityö, 88 s.
Tietoliikennetekniikka
Kesäkuu 2022

Tämän tutkielman tarkoitus on tutkia Turun yliopiston valmiutta vastata Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 eli yleisemmin Tietosuoja-asetuksen asettamiin haasteisiin henkilötietojen käsittelystä organisaation henkilörekistereissä. Tutkielmassa käydään läpi myös yleisemmin suuren organisaation haasteita suoriutua henkilötietojen käsittelystä asetuksen vaatimalla tavalla. Tutkielmassa keskitytään ensin käsittelemään yliopistoa organisaationa sekä sen luonnetta julkisena organisaationa sekä sen keskeisimpiä henkilörekistereitä. Näiden henkilörekisterien henkilötiedon käsittelyn analysoinnin kautta tutkielma pyrkii muodostamaan kuvan yliopistosta henkilötietojen käsittelijänä yleisemmin ilman, että läpikäynti ulotettaisiin jokaiseen organisaation henkilörekisteriin. Tutkielmassa käydään läpi Tietosuoja-asetuksen sisältö niiltä osin kuin sen katsotaan koskettavan tutkielmassa käsiteltäviä henkilörekistereitä. Lisäksi tutkielma keskittyy myös vertaamaan Tietosuoja-asetuksen sisältöä sen edeltäjään, vuonna 1995 julkaistuun Euroopan parlamentin ja neuvoston direktiiviin 95/46/EY. Lopuksi jokainen tutkielmaan valittu henkilörekisteri peilataan Tietosuoja-asetuksen vaatimuksiin ja analysoidaan niiden kyvykkyys vastata henkilötiedon käsittelylle asetettuihin vaatimuksiin laeissa ja asetuksissa. Osana analyysiä käydään läpi myös tutkimuksen aikana henkilötietojen käsittelyyn tehdyt kehitystoimet. Tutkimuksen teoreettinen osuus pohjautuu kokonaisuudessaan Tietosuoja-asetukseen ja sen pohjalta tehtyihin tietosuojaan liittyviin linjauksiin sekä tietosuojalakiin. Tutkielman tuloksena todetaan Turun yliopiston kyenneen vastaamaan Tietosuoja-asetuksen vaatimuksiin kaikkiaan hyvin, mutta tutkielman tuloksena syntyy myös lista henkilörekisterien puutteista ja kehitysehdotuksista kutakin henkilörekisteriä kohden.

Asiasanat: gdpr, tietosuoja, henkilötieto, henkilörekisteri

Sisällys

1 Johdanto

Tässä tutkielmassa tutkitaan Turun yliopiston ydinjärjestelmien kyvykkyyttä ja valmiutta vastata voimaan astuneen tietosuoja-asetuksen asettamiin tietosuojaa koskeviin haasteisiin. Tutkielmassa käyn läpi tietosuoja-asetuksen rakenteen siltä osin, mitä se koskettaa Turun yliopiston ydinjärjestelmiä ja peilaan sen jälkeen yliopiston järjestelmien valmiutta vastata tietosuoja-asetuksen vaatimuksiin, suosituksiin ja yleisemmin tietosuojan tilannetta rekistereissä.

Turun yliopisto on varsin suuri organisaatio Suomen mittakaavassa, sillä sen henkilöstön määrä on 3314 työntekijää (henkilötyövuotta, vuonna 2021) [1] ja opiskelijoiden määrä noin 22719 (vuonna 2021)[2]. Yliopisto toimii yliopistolain alla tarjoten julkisia palveluita, mitä kautta se on myös julkisoikeudellinen toimija ja julkisuuslain alla toimiva toimielin. Henkilörekisterien näkökulmasta tämä on luonnollisesti haastavampaa, kun julkisuuslain nojalla kaikki yliopiston toiminta on lähtökohtaisesti julkista, mutta henkilörekisterien ja henkilötietojen kannalta kaikki ei tietenkään voi olla julkista. Henkilörekisterien sisältöä ja henkilötietojen käsittelyä sääntelemään julkaistiin Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) joka astui voimaan 25.5.2018[3, artikla 99]. Tässä työssäni käytän direktiivistä sen yleisesti Suomessa käytettyä muotoa Tietosuoja-asetus. Julkisoikeudellisten toimijoiden lisäksi Tietosuoja-asetus kohdistui myös kaikkiin muihin henkilörekis-

tereihin Euroopassa; niin yksityisellä sektorilla kuin viranomaistenkin toiminnassa. Tietosuoja-asetuksessa määritetään henkilörekisterin pitäjän velvollisuudet kuin myös henilörekisterissä olevan yksilön oikeudet entistä tarkemmin ja asetuksen astuminen voimaan vaati monilta organisaatioilta entistä tarkempaa tarkastelua henkilörekisterien suojauksen, hallinnan, sijainnin ja rekisteriin pääsyn omaavien osalta.

Yliopiston ydintehtävinä on vapaan tutkimuksen ja tieteellisen sivistyksen edistäminen sekä tutkimukseen perustuvan ylimmän opetuksen antaminen [4, 3 §] ja näiden tehtävien kautta yliopistolla on erittäin suuri määrä erilaisia henkilörekistereitä hyvin erilaisiin tarpeisiin. Toisessa luvussa 2 tulen käsittelemään vielä tarkemmin yliopistoa organisaationa sekä sen organisatorista rakennetta. Käsittelen myös yliopiston henkilörekisterien rakennetta yleisellä tasolla sekä niiden liittymistä toisiinsa.

Tämän työn tutkimuskysymykseksi asetin seuraavat kysymykset: Tutkimuskysymys 1: Miten tarkastella ison organisaation GDPR:n mukaisuutta? Tutkimuskysymys 2: Mitä voidaan todeta Turun yliopiston keskeisten rekisterien tietosuoja-asetuksenmukaisuudesta?

Yllä esitettyjä tutkimuskysymyksiä lähdin tutkimaan tarkastelemalla rajattua määrää Turun yliopiston ydintoimintaan liittyvistä henkilörekistereistä, joissa mahdollisesti ilmenevät puutteet vaikuttaisivat eniten ja pahiten negatiivisesti yliopistoon. Tutkimuskymys 1:tä varten käyn luvussa viisi 5 läpi jokaisen tähän tutkielmaan mukaan otetun henkilörekisterin erikseen niiltä osin, kuin Tietosuoja-asetus kyseiseen henkilörekisteriin vaikuttaa. Tällä läpikäynnillä en voi täysin vastata asettamaani tutkimuskysymykseen, mutta koska kyseessä ovat yliopiston merkittävimmät ydinrekisterit, saan kattavan kuvan organisaation tavasta käsitellä henkilötietoja. Tämän läpikäynnin lopputulos vasta asettamaani tutkimuskysymykseen 2, eli havaitut puutteet ja niihin reagoiminen sekä rekisterinpitäjän vastuullisuuden arvioiminen vastaavat kysymykseen tietosuoja-asetuksen mukaisuudesta. Tutkielman

kolmannessa luvussa 3 käyn läpi tutkielmaan valikoituneet yliopiston henkilörekisterit niiden luonteen ja merkittävyyden kannalta. Tämän luvun tarkoitus on tarkastella näiden henkilörekisterien merkitystä yliopiston ydintoiminnassa. Tutkielman neljännessä luvussa 4 käyn läpi Tietosuoja-asetuksen sisällön niiltä osin kuin se koskettaa tutkielmaani valikoituneita henkilörekistereitä. Näiden lukujen avulla tutkielmani vastaa lopulta viidennessä luvussa asettamiini tutkimuskysymyksiin.

Tämän tutkielman tekemisen aloitin jo vuonna 2017 Turun yliopiston Tietohallinnon toimeksiannosta, mutta tutkielman valmistuminen venyi aina vuoteen 2022 saakka omien ajallisten haasteideni johdosta. Tästä syystä tutkielmassa kuvatut tietosisällöt ovat osin vanhentuneet, sillä esimerkiksi osa tutkielman ydinrekistereistä on jo siirretty toimimaan toisessa palvelussa. Näiden uusien palveluiden tietosuoja-asetuksen mukaisuutta en tässä työssä arvioi.

2 Yliopiston palvelut

2.1 Ydintoiminta

Yliopiston ydintoiminnasta on olemassa oma laki Suomen lainsäädännössä, yliopistolaki. Tuossa laissa määritetään yliopiston ydintehtävät: vapaan tutkimuksen sekä tieteellisen ja taiteellisen edistyksen edistäminen, tutkimukseen perustuvan ylimmän opetuksen antaminen sekä opiskelijoiden kasvattaminen palvelemaan isänmaata ja ihmiskuntaa [5, §2]. Turun yliopisto on määrittänyt johtosäännössään perustehtäväkseen vapaan tutkimuksen ja tieteellisen sivistyksen edistämisen sekä näihin liittyvän ylimmän opetuksen antamisen.[4, §3] Turun yliopiston strategia on olla korkealaatuista ja monialaista tutkimustyötä toteuttava kansainvälisesti kilpailukykyinen tiedeyliopisto, jossa toteutetaan vapaata tiedettä ja edistetään kansan sivistystä sekä tarjotaan niihin liittyvää ylintä opetusta. Yliopiston vaikutusalueen kehittäminen on myös yksi yliopiston strategisista tavoitteista.

2.2 Organisaatio

Turun yliopiston hallinto muodostuu hallituksesta, rehtorista, vararehtoreista ja yliopistokollegiosta.[4, §5] Lisäksi hallintoa edustavat eri palveluita tuottavat yksiköt ja palveluita tuottavien yksiköiden kokonaisuudet. Näitä yliopistolla ovat kehittämispalvelut, talouspalvelut, viestintä sekä yliopistopalvelut.[4, §18] Suurin osa yliopiston keskitetyistä palveluista on koottu yliopistopalveluihin erillisen palvelujohtajan alai-

suuteen. Vastaavasti taas yliopiston talouteen liittyviä palveluita hallinnoidaan kokonaisuudessaan talousjohtajan alaisuudessa toimivassa talouspalveluiden yksikössä. Varsinaista opetusta ja tutkimusta Turun yliopistossa suoritetaan tiedekunnissa, joita on yhteensä kuusi: humanistinen, kasvatustieteiden, lääketieteellinen, oikeustieteellinen, luonnontieteiden ja tekniikan sekä yhteiskuntatieteellinen tiedekunta. Näihin rinnasteisena Turun yliopistossa toimii aiemmin itsenäisenä korkeakouluna toiminut Turun kauppakorkeakoulu.[4, §6]

Turun yliopistossa lähes kaikki tietotekniset palvelut hallitaan keskitetysti yliopiston oman IT-palvelut -yksikön kautta ja toimesta. Vastaavasti kaikki muut yliopiston hallinnointiin liittyvä toiminnot hallitaan nykyisin keskitetysti omien palveluyksiköiden kautta ja toimesta. Palveluiden toteuttamisessa kaikki tietotekninen osaaminen on pyritty keskittämään IT-palveluihin, kuitenkin niin, että käyttäjien tukemiseen tarvittava tekninen pääkäyttäjätuki on voitu jättää edelleen suurelta osin muihin palveluyksiköihin. Muita keskitettyjä palveluita yliopistopalveluissa ovat esimerkiksi henkilöstöpalvelut, hyvinvointipalvelut, kirjasto, lähipalvelut, toimitilapalvelut sekä koulutuksen toimiala. Näistä tämän tutkimuksen kannalta merkittävimpiä palveluyksiköitä ovat IT-palveluiden ohella henkilöstöpalvelut sekä koulutuksen toimiala, joiden keskeisimpiin rekistereihin tutkimuksessa keskityn.

IT-palvelut ylläpitävät siis palveluyksiköiden käyttämiä järjestelmiä. Vastaavasti palveluyksiköt itse vastaavat palveluidensa käyttäjäkoulutuksista käyttöoikeuksien hallinnoinnista sekä yhteydenpidosta palvelun mahdolliseen yliopiston ulkopuoliseen toimittajaorganisaatioon itse palvelun osalta, teknisistä asioista kommunikoitaessa IT-palvelut luonnollisesti toimivat konsultoitavana palveluyksikkönä. Niiltä osin, kun ylläpito koskettaa järjestelmien asentamista yliopiston omaan konesaliympäristöön yliopiston omille palvelinlaitteille, virtuaalisille tai fyysisille palvelinlaitteistoille. IT-palvelut hallinnoi myös yliopiston verkkoympäristöä, jossa palveluita pääsääntöisesti käytetään. Palveluiden hallittu käyttö vaatii tuekseen myös hyvin hal-

linnoitua käyttäjähallintaa, niin yliopiston tunnushallinnan osalta kuin palveluiden käyttöoikeushallinnoinnin osalta. Tunnushallinta yliopistolla on keskitetty identiteetinhallinnan palvelun alle, jossa jokaiselle käyttäjälle annetaan vain ja ainoastaan yksi identiteetti, jolloin käyttäjän identiteetti on aina tiedossa ja tunnettu. Käyttäjällä voi sen sijaan olla erilaisia rooleja yliopistossa ja näitä eri rooleja hallinnoidaan yhtälailla identiteetinhallinnan palvelussa. Kaikki palvelut yliopistolla eivät hyödynnä keskitettyä roolien hallintaa, vaan osassa palveluista käyttäjähallinnointi tehdään itsenäisesti palvelun sisään rakennetulla käyttäjä- ja rooli- tai käyttäjäryhmähallinnalla. Ne palvelut, joissa roolipohjainen hallinnointi on toteutettu keskitetyn käyttäjähallinnan kautta saavuttavat käyttöoikeuksien päivittymisen suhteen etua manuaalisesti hallinnoituihin verrattuna.

2.3 Rekisterit Turun yliopistossa

Turun yliopiston palveluiden hallinta rakentuu hyvin pitkälti erilaisten rekisterien varaan, kuten monessa muussakin organisaatiossa nykyään. Tietoyhteiskunnan vaatimukset ovat ajaneet organisaatiot siihen, ettei ilman tietoteknisiä järjestelmiä ja rekistereitä nykyorganisaatioiden tarjoamien palveluiden olisi juuri mahdollista edes toimia. Lähes jokainen palvelu tänä päivänä pitää sisällään jonkinlaisen rekisterin, eli käyttäjätietokannan, jossa rekisteröidyistä listataan erilaisia asioita aina tarpeen mukaan. Eri palveluiden rekisterit on rakennettu hyvin erilaisin tavoin ja rekisterin rakenne ja toimintaperiaate riippuvatkin hyvin usein palvelun kehittäjästä sekä käytetyn teknologian tarjoamista mahdollisuuksista ja asettamista rajoitteista. Eri palvelut toimivat hyvin usein myös erilaisilla käyttöjärjestelmäalustoilla tai nojautuvat erilaisiin palvelinalustaratkaisuihin, jolloin myös rekisterien toimintaperiaate on useimmiten hyvin erilainen. Usein rekisterit on myös rakennettu täyttämään jonkin erityisen tarpeen ja jokaisen rekisterin rakentamisessa ei ole välttämättä osattu ottaa myöskään huomioon ajankohtaista lainsäädäntöä. Siksi ratkaisu on saattanut

jo valmistuessaan rikkoa rekisterien pitämiselle asetettuja vaatimuksia, velvoitteita tai lakeja. Myös lainsäädäntö on saattanut muuttua sen jälkeen, kun rekisterin tekninen pohjaratkaisu ja toimintaperiaatteet on luotu, eikä rekisterin rakennetta tai toimintalogiikkaa ole mitä todennäköisimmin huomattu tai katsottu tarpeelliseksi muuttaa, vaikka lakimuutos sitä olisikin edellyttänyt.

Turun yliopiston yhteisessä käytössä olevien rekistereiden keskeinen yhdyspiste on identiteetinhallintajärjestelmä, IDM. Jokainen Turun yliopiston IT-palveluiden käyttäjä on rekisteröity keskitettyyn käyttäjärekisteriin, jossa hallinnoidaan hänen identiteettiään. Identiteetinhallintajärjestelmässä ylläpidetään kaikkia yliopistolla jossakin vaiheessa käytössä olleita käyttäjiä ja heidän perustietojaan. Itse IDM on kuitenkin vain tietoja kokoava piste. Varsinaisena identiteettien lähdejärjestelmänä toimivat tässä työssä myöhemmin tarkemmin käsiteltävät erilliset henkilöstörekisteri sekä opiskelijarekisteri. IDM toimii myös pääsynhallinnan keskeisenä rekisterinä ja ohjaa edelleen tietoja käyttäjistä varsinaista käyttäjien pääsynhallintaa toteuttaviin rekistereihin, Active Directoryyn (AD) sekä Lightweight directory Access Protocol (LDAP) -käyttäjähakemistoon. IDM toimii myös keskeisessä roolissa siinä mielessä, että identiteetinhallinnan ominaisuudessa rekisteri välittää muihin rekistereihin tietoa, missä roolissa tai rooleissa käyttäjä Turun yliopistossa toimii. Tähän rooliin voidaan näin sitoa myös suoraan henkilön pääsyoikeuksia eri rekistereihin ja välittää tämä roolitieto rekistereille Open source Access Managemenst (OpenAM) -kertakirjautumispalvelun kautta.

Keskitetyt rekisterit Turun yliopistossa hyödyntävät lähes poikkeuksetta kaikki edellä esitettyjä identiteetin- ja pääsynhallinnan työkaluja ja palveluita. Erilaisia rekistereitä Turun yliopiston kokoisessa organisaatiossa on jo yksistään keskitetyssä käytössä kymmeniä erilaisia, ja niiden avulla mahdollistetaan yliopiston ydintoimintojen toteuttaminen ja tarjotaan työntekijöille, opettajille ja tutkijoille heidän työssään tarvitsemat työkalut ja toisaalta opiskelijoille heidän opiskelujensa edistämisen

mahdollistavat sähköiset työkalut.

Turun yliopistossa jokainen palveluyksikkö käyttää pääsääntöisesti omaa, kohdennettuun tarpeeseen hankittua ja määritettyä järjestelmää. Osa järjestelmistä on olemassa, koska laki määrää yliopistoa tekemään tutkimaan tai opettamaan tai esimerkiksi raportoimaan näihin liittyviä asioita toiminnastaan. Osa palveluista ja järjestelmistä taas on olemassa yksinkertaisesti toiminnan mahdollistamiseksi tai helpottamiseksi. Tästä syystä myös yliopistossa käytössä olevat rekisterit poikkeavat toisistaan hyvin paljon juuri olemassaolonsa perustan näkökulmasta tarkasteltuna. Turun yliopistossa on aktiivisessa työsuhteessa 3314 työntekijää (henkilötyövuotta, vuonna 2021) [1], joiden tietojen hallinnoimiseen tarvitaan henkilörekisteri esimerkiksi työsuhteiden tyypin, palkka-asioiden, esimiestietojen ynnä muiden asiaan liittyvien tietojen taltioimiseen ja hallinnointiin.

Pääasiallisesti yliopiston rekisterit sijaitsevat yliopiston omassa palvelinkeskuksessa ja pääasiallisesti palvelut toimivat yliopiston omistamalla virtuaalipalvelinalustalla. Näin ollen myös rekisterien tietoturva teknisestä näkökulmasta tarkasteltuna on yliopiston itse hallinnoima ja ylläpitämä.

Keskitettyjen rekisterien lisäksi Turun yliopistossa on suuri joukko muita rekistereitä, joita on syntynyt aikojen saatossa erilaisiin tarpeisiin yliopiston tiedekuntien, laitosten, yksiköiden tai yksittäisten työntekijöiden tarpeisiin. Tällainen rekisteri saattaa olla yksikön tarpeeseen tehty yksinkertainen tai monimutkaisempikin järjestelmä tai vain tarpeeseen koottu joukko tietoja esimerkiksi viestinnällisiin tai markkinoinnin tarpeisiin. Tämän tyyppinen koostettu lista henkilöitä muodostaa henkilörekisterin, mikäli siinä on käytetty henkilön yksilöivää tunnistetietoa, jollaisen tällainen lista hyvin usein sisältää.[6, s. 2] Esimerkiksi listaan liitetty tieto henkilön sähköpostiosoitteesta on jo riittävä yksilöivä tieto ja tekee listasta henkilörekisterin.

Osa yliopiston henkilörekistereistä siis muodostavat muista yliopiston järjestelmistä, eli niin sanotuista lähdejärjestelmistä siirretyt tai haettavat tiedot. Osan re-

kistereistä taas muodostavat yksittäiset henkilöt omilla toimillaan, kun he keräävät toisten henkilöiden tietoja listaksi ja tallentavat tällaisen jollekin tallennusratkaisulle: verkkolevylle, omalle työasemalleen, siirrettävälle tallennusalustalle, kuten muistitikulle. Näiden lisäksi yliopistolle syntyy henkilörekistereitä, kun yliopiston ulkopuolella olevista lähderekistereistä siirretään henkilötietoja yliopiston palveluiden ja järjestelmien käyttöön. Nämä rekisterit on hyvä eritellä omaksi kokonaisuudekseen, koska vastuu näiden rekisterien sisällön oikeellisuudesta ei ole yliopistolla itsellään, vaikka rekisterinpitäjän ominaisuudessa lopullista vastuuta kantaakin yliopisto itse, tai oikeammin rekisterinpitäjäksi merkitty taho yliopistolla.

3 Tutkimukseen valittujen rekisterien tarkastelu

Tutkimukseni kohteeksi olen valinnut neljä eri tyyppistä henkilörekisterikokonaisuutta Turun yliopiston henkilörekisterien joukosta. Valinnan kohteella on jokin erityinen asema tai ominaisuus erilaisten rekisterien joukossa tai henkilörekisterin asema yliopistolla on muutoin jollakin tavalla erityinen. Tutkittavista henkilörekistereistä kolme toimii yliopiston henkilötietojen lähdejärjestelmänä, eli kyseisistä kolmesta henkilörekisteristä tuotetaan niin kutsuttua metadataa, eli lähdeaineistoa henkilöistä muiden järjestelmien ja rekisterien käyttöön. Nämä kolme henkilörekisteriä ovat Turun yliopiston opiskelijatietorekisteri, henkilöstörekisteri sekä kontaktirekisteri. Neljäs tutkittava rekisteri taas on Turun yliopiston tietovarasto, Data Warehouse, joka toimii raportointipalveluna ja eri rekisterien tietoja yhdistävänä ja kokoavana keskitettynä rekisteripalveluna yliopiston käyttäjille. Erityisluonteet rekistereissä käyn tarkemmin läpi kunkin rekisterin kohdalla erikseen, mutta pääasiallisesti tarkastellaan lakisääteisten rekisterien ja toisaalta poistumassa olevien rekisterien erityisasemaa Euroopan Unionin 25.5.2018 voimaan astuvan [3, artikla 99]Tietosuoja-asetuksen näkökulmasta. Rekistereistä käyn läpi niitä seikkoja, joilta osin Tietosuoja-asetus edellyttää henkilörekistereitä tarkastelemaan, ja joilta osin asetus henkilörekistereihin vaikuttaa.

3.1 Opiskelijatietorekisteri

Turun yliopiston opiskelijatietorekisteri elää tällä hetkellä murroksen vaihetta. Uutta järjestelmää ollaan kehittämässä ja ottamassa vaiheittain käyttöön, mutta suurimmalta osin käyttöönotto tullee siirtymään vielä pitkän ajan päähän. Nykyisen järjestelmäkokonaisuuden ydin on alun perin rakennettu toisen korkeakoulun, Tampereen yliopiston toimesta ja sittemmin otettu käyttöön myös Turun yliopistossa. Sen jälkeen järjestelmäkokonaisuutta on laajennettu ja kehitetty palasina osin Tampereen yliopiston toimesta, mutta paljolti myös Turun yliopiston oman ohjelmointityön tuloksena. Nykyisessä järjestelmäkokonaisuudessa on erotettavissa viisi erillistä kokonaisuutta: keskitettynä tietokantana toimiva Opsu, sen pääasiallisena käyttöliittymänä toimiva Nettiopsu, opiskelijoiden henkilökohtaisten opintosuunnitelmien rakentamisen käyttöliittymä Hops, opettajien käyttöliittymänä opintojen suunnitteluun tarkoitettu Opsi sekä Opinto-opas, josta opiskelija löytää tiedot eri tiedekuntien kursseista. Tämän lisäksi Turun yliopiston alaisuudessa toimiva Avoin yliopisto käyttää samaa keskustietokantaa, Opsua, mutta itse rekisterin käyttöön heillä on erillinen käyttöliittymänsä.

Turun yliopiston opiskelijatietojärjestelmään rekisteröidään tutkinto- ja erillisopiskelijoiden henkilö- ja opintotiedot opintojen seuraamista ja opintojen tarkoituksenmukaista tarjoamista varten. Rekisterin olemassaolo perustuu siihen, että opintohallinnollisten tehtävien hoitaminen ja opetuksen ja oppimisen suunnittelu edellyttävät tällaisen rekisterin olemassaoloa, jotta opiskelijatietojen rekisteröinti olisi mahdollista. Näiden tehtävien perustana on yllä esitetyn yliopistolain (645/1997) lisäksi yliopistoasetus (115/1998). Toissijainen tehtävä opiskelijatietojärjestelmällä on toimia näiden opiskelijan opintosuoritusten arkistointipaikkana. Opintosuoritusten arkistointi on Arkistolaissa (831/94) ja Turun yliopiston arkistonmuodostussuunnitelmassa määritetty pysyvästi säilytettäviksi [7, §8].

Opiskelijatietorekisteriä Turun yliopistossa käyttävät kaikki sellaiset henkilöt,

joiden työnkuvaan opiskelijatietojen ja opintosuoritusten merkitseminen, muokkaaminen tai muu käsittely kuuluu. Käyttöoikeudet palveluun anotaan erillisellä käyttölupahakemuksella. Käyttölupahakemukset käsitellään palvelun pääkäyttäjän toimesta. Hän myös myöntää tarvittavan laajuiset käyttöoikeudet palveluun ja arkistoi myös käyttölupahakemuksen Turun yliopiston arkistonmuodostussuunnitelman mukaisesti. Käyttöoikeuksia annetaan anotun mukaisesti, kuitenkin tarkastellen anojan toimenkuvaa yliopistolla niin, että käyttöoikeudet palveluun annetaan anojalle todetun tarpeen mukaisesti. Käyttölupa anotaan paperisella lomakkeella, jota säilytetään yksikössä arkistonmuodostussuunnitelman mukaisesti.

Opiskelijatietorekisteri sijaitsee Turun yliopiston keskitetyllä virtuaalipalvelinalustalla sijaitsevalla palvelimella. Opsu -rekisteri on hyvin keskeisessä asemassa palvelussa; sen ympärille rakentuvat kaikki muut palvelun liitännäisosat ja se toimii kaiken tiedon varsinaisena tallennuspaikkana. Opsu -keskusrekisterin käyttöliittymä on komentorivipohjainen ja itse keskusrekisteriä käyttää vain hyvin harva käyttäjä koko Turun yliopistosta. Opiskelijatietorekisteri toimii siis kaiken oppimistiedon aktiivisena tallennuspaikkana, mutta myös arkistona kaikista menneistä opintosuorituksista, kurssimerkinnöistä ja opiskelijoista. Opsu toimii siis tallennuspaikkana sekä Turun yliopiston varsinaisten opiskelijasuoritusten ja -tietojen osalta, mutta myös yliopiston järjestämien erillisopintojen osalta. Erillisopinnot tarkoittavat opintoja, joita Turun yliopistossa suorittavat sellaiset opiskelijat, joilla ei ole varsinaista tutkinnonsuoritusoikeutta tai jotka suorittavat vain jonkin opintojakson tai opintokokonaisuuden. [8] Näiden lisäksi Opsua keskusrekisterinään käyttää myös Turun yliopiston Avoimen yliopiston opintoja tarjoavat yksiköt.

Opiskelijatietorekisteriin tallennetaan opiskelijasta hyvin tarkkaan yksilöiviä tietoja, koska opinnot tulee aukottoman varmasti saada kohdistettua juuri oikealle henkilölle. Tämän vaatimuksen asettaa laki, sillä yliopistolla on velvollisuus arkistoida esimerkiksi opiskelijan tutkintoon liittyvät yksityiskohtaiset tiedot pysyvästi samoin

kuin opiskelijasuoritukset ja opiskeluoikeuksiin liittyvät tiedot ja opiskelijavaihtoihin liittyvät tiedot. [7, §8] Rekisterissä säilytettävän tiedon luonne ei ole kovin arkaluontoista, mutta toki henkilöstä järjestelmässä säilytettävät tiedot asettavat rekisterin suojaukselle hyvin tarkat vaatimukset. Opiskelijatietorekisterissä käyttöoikeuksia hallinnoidaan yksinomaan pääkäyttäjien toimesta. Käyttöoikeudet rekisterissä annetaan suoraan tietokantaan kytkeytyvällä käyttöliittymällä. Käyttöoikeustasoja on kaikkiaan 21 erilaista. Näillä eri tasoilla määritetään käyttäjille eri osiin Opsua ja sen liitännäispalveluita luku- ja kirjoitustason oikeuksia aina kulloisenkin käyttäjän tarpeen mukaisesti. Haasteena käyttöoikeuksien määrittelyssä on tunnistettu niiden sidonnaisuus pelkästään käyttäjän UTU-tunnukseen, jolloin esimerkiksi työsopimuksen päättyessä saattaa käyttäjälle jäädä liian laajat käyttöoikeudet opiskelijatietorekisteriin tai sen liitännäiseen palveluun. Järjestelmän käyttöoikeuksia anotaan erillisellä kirjallisella lomakkeella ja käyttöoikeudet arvioidaan vielä pääkäyttäjien toimesta ennen oikeuksien antamista. Käyttäjän sopimuksen, työsopimuksen tai siihen rinnastettavan sopimussuhteen, päätyttyä sen sijaan pääkäyttäjä ei saa välittömästi tietoa sopimuksen päättymisestä ja näin käyttöoikeudet voivat jäädä järjestelmään voimaan vielä merkittäväksi aikaa. Näin on potentiaalinen riski syntyä tietoturvaloukkaukselle altis tilanne, jossa rekisteröityjen tietoja on sellaisen henkilön saatavilla, jolla ei näihin tietoihin tulisi enää pääsyä olla.

Henkilörekisterin sisältö määräytyy hyvin pitkälti opiskelijan itse tuottamana, eli rekisterin pohjatiedot ja varsinaiset henkilötiedot muodostuvat opiskelijan itsensä antamina opintojen alussa. Vastaavasti tietojen päivittämisestä vastaa opiskelija itse tietojen muuttuessa. Opiskelijan opintotiedot taas kertyvät rekisteriin sitä mukaa, kun opiskelija esimerkiksi suorittaa kursseja tai opintokokonaisuuksia Turun yliopistossa tai vain ilmoittautuu yliopistossa läsnä olevaksi opiskelijaksi. Rekisteristä ei tietoa pääsääntöisesti poisteta, ellei poistamiselle ilmene erityistä tarvetta. Näissäkin poistamisissa lainsäädäntö asettaa kuitenkin poistolle rajoitteet. Tieto-

jen poistamiseen rekisteristä ei kuitenkaan ole oikeuksia kuin erikseen määritetyllä käyttäjäryhmällä.

Opiskelijatietorekisteristä lähetetään edelleen tietoja yliopiston sisäiseen käyttöön toisiin rekistereihin, kuten yliopiston tietovaraston, yliopiston kirjaston tietojärjestelmän, käyttäjähallinnan, yliopiston intranetin henkilöhaun ja muutamien muiden rekisterien tai palveluiden käyttöön. Tämän lisäksi opiskelijoiden suorittamista opinnoista tehdään raportointia ja opiskelutietoja välitetään edelleen käytettäväksi lakisääteisistä vaatimuksista Korkeakoulujen yhteisten opiskelijapalveluiden, Opiskelijavalintarekisterin, Opetus- ja kulttuuriministeriön, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviran, Tilastokeskuksen, Ylioppilaiden terveydenhoitosäätiön, sekä joidenkin muiden pienempien toimijoiden tai palveluiden käyttöön. Kolmansiin maihin tietoja rekisteristä ei luovuteta. [9]

Opiskelijatietorekisterin edeltäjästä on aikanaan kaikki opiskelijatiedot siirretty hallitusti nykyisen rekisterin sisään. Vanhaa rekisteriä ei enää ole säilytetty, vaan siellä ollut arkistoitava aineisto on tallennettuna nykyiseen rekisteriin. Tutkimusaineistoa tätä tutkimusta varten kerätessäni sain selville, että avoimen yliopiston edeltänyt opiskelijatietorekisteri sen sijaan on vielä olemassa paikallisena asennuksena kaikkiaan kuudella yliopiston omistamalla työasemalla. Myös opiskelijatietorekisterin tietokanta sijaitsee paikallisena kopiona kyseisillä työasemilla. Keskitetty tietokanta sen sijaan on siirretty osaksi Turun yliopiston nykyistä opiskelijatietorekisteriä, kun avoin yliopisto kokonaisuudessaan siirtyi myös sitä käyttämään. Paikallisia kopioita avoimen yliopiston opiskelijatietorekisteristä on säilytetty, koska siellä olleita tietoja on jouduttu vuosien saatossa vielä etsimään opiskelijoilta tulleiden tietopyyntöjen johdosta.

3.2 Henkilöstörekisteri

Turun yliopiston henkilöstörekisterinä toimii Aditro Oy:n toimittama Personec F -järjestelmä. Henkilöstörekisteri on vastaavasti kuin opiskelijatietorekisterikin kokemassa vastaavan muutoksen, eli järjestelmävaihdos on jo suunnitteilla. Vastaavasti kuin opiskelijatietorekisterikin, Personec F tulee olemaan Turun yliopiston käytössä vielä toistaiseksi. Henkilöstöjärjestelmiin luetaan yliopistolla kuuluviksi myös Personec HR sekä Personec ESS, joista Personec HR:ssä suoritetaan henkilöstön palkkatason arvioinnit sekä tallennetaan kehityskeskustelulomakkeet. Personec ESS taas keskittyy henkilöstön lomien hallinnointiin, kuten anomiseen ja hyväksyntään. Näistä järjestelmistä keskityn tutkimuksessani kuitenkin ainoastaan Personec F -järjestelmään, jossa hallinnoidaan ja säilytetään henkilöstön työsuhdetietoja, palkkatietoja sekä henkilöstön lisäksi yliopistolta palkkioita saavien henkilöiden henkilötietoja. Henkilöstörekisterin olemassaolon perusta on henkilöstöhallinnon ja palvelussuhdeasioiden hoitaminen sekä työnantajatehtävien ja -velvoitteiden hoitaminen. Näiden tehtävien ja velvoitteiden hoitaminen Turun yliopiston kokoisessa organisaatiossa olisi mahdotonta. Lisäksi yliopisto työnantajana on velvoitettu arkistoimaan työsuhdetietoja ja esimerkiksi palkkatietoja yliopiston arkistonmuodostussunnitelmassa määritetyn ajan. Tätä arkistointia suoritetaan ensisijaisesti henkilöstöjärjestelmässä.

Personec F henkilöstörekisteri sijaitsee järjestelmää yliopistolle toimittavan toimittajaorganisaation tiloissa yliopiston tietoverkon ulkopuolella. Järjestelmän käyttö on mahdollista ainoastaan yliopiston verkosta - joko suoraan yliopiston tietoverkkoon kytketyllä työasemalla tai etäkäyttöratkaisujen avulla käyttäen Turun yliopiston käyttäjätunnusta ja salasanaa.

Henkilöstörekisterin luonne on jo lähtökohdiltaan sellainen, että sen sisältämä tietosisältö on hyvin sensitiivistä. Järjestelmän henkilörekisteriin tallennetaan rekisteröidyistä heidän työsuhdetietojaan, tietoja entisistä työsuhteista, palkkatietoja

sekä luonnollisesti myös hyvin yksilöiviä tietoja. Varsinaisesti arkaluontoiseksi luokiteltavaa tietoa rekisteri ei kuitenkaan sisällä, vaikka rekisteröidystä tallennetaan myös esimerkiksi sairauspoissaolotietoja - poissaolon syytä ei kuienkaan rekisteriin tallenneta. Johtuen yliopiston toiminnan luonteesta viranomaisorganisaationa, on suurin osa rekisterin sisältämästä henkilötiedosta kuitenkin julkisuuslain nojalla julkista tietoa. Rekisterissä on kuitenkin myös salaiseksi luokiteltuja tietoja, joita taas ei anneta julkisesti nähtäväksi.

Henkilöstörekisteriin on käyttöoikeudet ainoastaan niillä henkilöillä, joilla työtehtäviensä vuoksi tulee olla pääsy rekisteriin tallennettuihin tietoihin. Käyttöoikeuksien hallinta tapahtuu järjestelmässä itsessään. Järjestelmän tunnistautuminen tapahtuu yliopiston myöntämällä käyttäjätunnuksella ja salasanalla, joita hallinnoidaan yliopiston identiteetinhallintajärjestelmässä. Jokaisella Turun yliopiston henkilökuntaan kuuluvalla on oikeus päästä järjestelmään tarkastelemaan omia tietojaan. Lisäksi, mikäli henkilöllä on alaisia, päästä katsomaan myös alaisten tietoja.

Rekisterin sisältö koostuu kokonaisuudessaan henkilön työsopimukseen kirjatuista tiedoista, tai työsuhteeseen, palkkaan tai palkkioihin liittyvistä tiedoista, jotka järjestelmään saadaan henkilöltä itseltään. Henkilön verotukseen liittyvät tiedot rekisteriin saadaan verottajalta. Mikäli rekisteröidystä tallennetaan tutkintotietoja, saadaan ne joko henkilöltä itseltään tai yliopiston opintorekisteristä. Tietojen päivittäminen reksiteriin niiden muuttuessa tehdään rekisteröidyn itsensä toimesta tai esimerkiksi palkkojen tai palkkioiden osalta esimieheltä tai yliopiston muusta järjestelmästä saatavan tiedon perusteella. Rekisteristä ei poisteta henkilöitä työsuhteen päättyessä lakisääteisten säilytysvelvollisuuksien täyttämisen vuoksi.

Henkilöstörekisteristä lähetetään edelleen tietoja yliopiston sisällä toisiin rekistereihin, kuten yliopiston identiteetinhallintajärjestelmään, tietovarastoon sekä henkilöstöjärjestelmän yhteydessä toimiviin, edellä esiteltyihin Personec HR ja ESS -järjestelmiin. Tietovaraston kautta rekisteröidyn tietoja lähetetään edelleen myös

yliopiston intranet-palveluun, työaikakirjausjärjestelmään, yliopiston tutkimustietojärjestelmään, yliopiston työaikaleimausjärjestelmään sekä yliopiston toiminnanohjausjärjestelmään. Yliopiston ulkopuolelle rekisterin tietoja lähetetään viranomaistahoille, kuten verottaja, eri ministeriöt, sekä eläkevakuutuslaitoksille, työterveysyhteistyökumppanille, palkanmaksua hallinnoivalle organisaatiolle ja muille lain edellyttämille yhteistyötahoille. ETA -alueen ulkopuolelle rekisterin tietoja ei luovuteta. [10]

Rekisterin käyttäjähallinta on hyvin harvojen pääkäyttäjien hallinnoima ja pohjautuu hyvin pitkälti manuaaliseen ylläpitoon. Hallinnoinnin voidaan kuitenkin katsoa olevan hallittua, koska pääkäyttäjät saavat tiedon muutoksista esimerkiksi käyttäjien työrooleissa suoraan järjestelmästä itsestään, jolloin muutos on mahdollisimman tuoretta. Manuaaliseen ylläpitoon liittyy kuitenkin aina omat riskinsä ja siksi järjestelmän käyttäjähallinnan voidaan katsoa olevan pienoinen ongelma rekisterin tietosuojan kannalta.

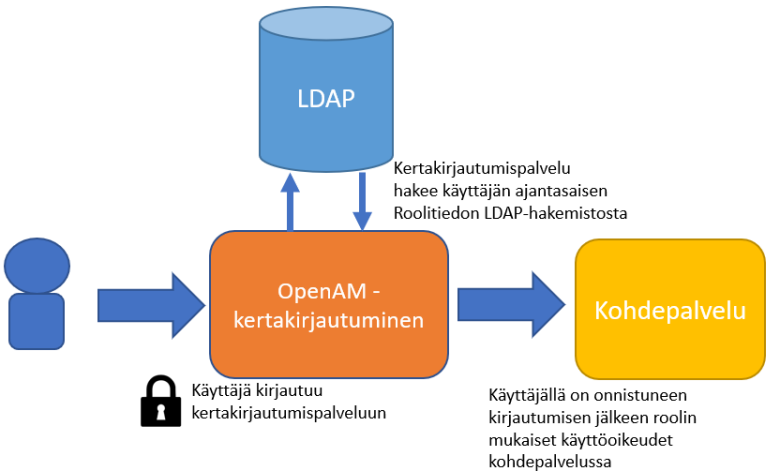
3.3 Kontaktirekisteri

Turun yliopiston kontaktirekisteri on osa vuonna 2012 yliopistolle hankittua tapahtuman- ja kontaktinhallinnan järjestelmää, Konstaa. Turun yliopistolla on yksiköissä myös muita asiakas- ja kontaktirekistereitä, mutta tässä tutkimuksessa keskityn nimenomaan yliopiston keskitetyksi kontaktirekisteriksi hankittuun kontaktirekisteriin sekä sen yhteydessä toimivaan tapahtumanhallintajärjestelmään. Kontaktirekisteri on Turun yliopiston merkittävin työkalu toteutettaessa yliopiston kolmatta päätehtävää, yhteiskunnallista vuorovaikutusta. Yliopiston kontaktirekisteri on toistaiseksi ollut aktiivisessa käytössä vain hyvin marginaalisella käyttäjäryhmällä ja siksi kontaktihenkilöiden määrä rekisterissä ei vielä kata kaikkia yliopiston yhteiskunnallisia yhteistyötahoja. Kontaktinhallinta kokonaisuudessaan on yliopistolla ollut aina hyvin aktiivista, mutta keskitetyn kontaktirekisterin muodossa kontaktinhallinta on

vielä hyvin pienimuotoista. Merkittävimmän osan kontaktirekisteristä muodostavat tällä hetkellä yliopiston alumnit, joita rekisterissä onkin yli 13700 rekisteröityä (vuonna 2020). Rekisteriin alumneja on kerätty jo pitkään ennen nykyistä järjestelmäkokonaisuutta. Konsta-järjestelmän edeltäjästä Prospektista siirrettiin Konstan käyttöönoton yhteydessä noin 7200 rekisteröidyn verran. Tämän jälkeen kontaktirekisterien alumniksi on voinut rekisteröityä itse erillisellä rekisteröitymislomakkeella. [11] Maisteri-tutkinnon suorittaneilla, eli tutkinnon suorittaneilla Turun yliopiston opiskelijoilla on lisäksi ollut mahdollista valmistumisensa jälkeen liittyä alumniksi. Tähän suostumuksensa antaneet on valmistumisen yhteydessä siirretty automaattisesti osaksi yliopiston kontaktirekisteriä.

Toinen osa Konsta-järjestelmää on tapahtumanhallinta. Tapahtumanhallintaan on oikeus perustaa tapahtumia kenen tahansa Turun yliopiston henkilökuntaan kuuluvan tai siihen rinnastettavan. Tapahtumanhallinnalla hallinnoidaan tapahtuman ilmoittautumisia, tarvittavien yhteystietojen kerääminen, tapahtumaan liittyvät mahdolliset lisäkysymykset sekä tapahtuman ilmoittautumismaksujen kerääminen ja tapahtumaan liittyvän viestinnän mahdollistaminen. Tapahtumia Konsta-järjestelmään perustettiin esimerkiksi vuoden 2017 aikana lähes 600 kappaletta ja Konstan kautta yliopiston järjestämiin erilaisiin tapahtumiin ilmoittautui kaikkiaan lähes 19000 osallistujaa.

Kolmantena isompana kokonaisuutena Konsta-palvelussa on syytä mainita yliopiston henkilökunnan sisäisten koulutusten hallinnoinnin kokonaisuus. Tämä Henkilöstön kehittämisen koulutushallinta pitää sisällään erilliset toteutukset Konsta-palvelun kahdesta peruskomponentista, eli erillisen tapahtumanhallinnan ja kontaktirekisterin yliopiston henkilökunnan osalta. Yliopiston henkilökunta on myös osa Konstan kontaktirekisteriä, sillä näin palvelussa on pyritty mahdollistamaan henkilökunnan työ- ja yksityisidentiteettien eriyttäminen omiksi kokonaisuuksikseen. Henkilöstön kehittämisen koulutus- ja henkilöstöhallintaan on pääsy ainoastaan ra-



Kuva 3.1: Kuvaus SSO-kertakirjautumisesta kohdepalveluun

jallisella määrällä käyttäjiä. Käytännössä niillä, jotka sisäisiä koulutuksia organisoivat ja järjestävät.

Konsta-palvelu sijaitsee Turun yliopiston omalla virtuaalialustalla sijaitsevalla virtuaalipalvelimella. Järjestelmä pohjautuu DotNetNuke:n (DNN) avoimen lähdekoodin julkaisujärjestelmään ja käyttää SQL-tietokantaa tietokantaratkaisunaan. Käyttäjien kirjautuminen palveluun tapahtuu Turun yliopistossa käytössä olevalla OpenAM (Open access management) kertakirjautumisjärjestelmällä.3.1 Järjestelmään on sallittu kirjautuminen vain UTU-tunnuksen omaavilta käyttäjiltä ja autentikointipalvelun hyödyntäessä Turun yliopiston kirjautumiskäytänteitä, ei erillistä salasanahallintaa itse palvelussa tarvita. Järjestelmä mahdollistaa kuitenkin myös paikallisen autentikoinnin, jolloin kertakirjautumisjärjestelmän vikaantuminen ei lamaannuta palvelua kokonaan. Konsta-palvelun toimittaa Turun yliopistolle eTaika Oy, joka on myös itse toteuttanut koko palvelun rakentamisen. Ylläpito tietokanta- ja sovelluspalvelimelle tapahtuu Turun yliopiston referenssiarkkitehtuurin mukaisella tavalla tietoturvallisesti.

Kontaktirekisteri sisältää hyvin paljon henkilötietoa jo rekisterin luonteestakin johtuen. Rekisterissä on kuitenkin pyritty minimoimaan perinteisesti sensitiivisek-

si tiedoksi miellettävien tietotyyppien tallentamista kuten rekisteröidyn henkilötunnusta. Rekisteri koostuu yhteisessä käytössä olevista kontaktin perustiedoista ja erikseen käyttöoikeuksin suojatuista roolitiedoista, joista Konsta-järjestelmässä käytetään nimitystä profiili. Rekisteröidyn yleistiedot, kuten nimi, yhteystiedot, mahdolliset yritystiedot ja tieto työtehtävistä sekä sukupuoli- ja syntymäaikatiedot. Suurimmalta osin rekisterin tietosisältö on rekisteröidyn itsensä antamaa, pakollisia tietokenttiä ei kontakteille ole asetettu. Rekisteröityyn liitetty rooli, eli profiili voi pitää sisällään mitä tietoa tahansa. Rooliin määritetään rekisteröityyn liittyvää yksilöllistä erityistietoa, jonka perusteella häneen voidaan esimerkiksi kohdistaa myös yksilöllisiä toimenpiteitä tai kohdennettua viestintää. Rekisteröidyn on mahdollista itse korjata hänestä kerättäviä tietoja, mikäli hänelle lähetetään tätä varten muodostettu erillinen linkki. Rekisteröity voi samalla myös poistaa itseään koskevan roolin tai muuttaa sitä, mikäli rooli on määritetty väärin tai henkilö ei enää tahdo itseään roolin kautta yksilöitävän. Varsinaisesti arkaluontoiseksi määriteltävää tietosisältöä ei rekisteröidystä kuitenkaan rekisteriin kerätä.

Tapahtumanhallintaa voidaan pitää käytännössä kokoelmana useita pieniä erillisiä henkilörekistereitä. Koko Turun yliopiston henkilökunnalla on pääsy kaikkiin tapahtumanhallinnassa oleviin tapahtumiin mukaan lukien tapahtuman osallistujalistat, eli rekisteröidyt. Tapahtuma on kuitenkin ollut mahdollista suojata näkyväksi vain määritellylle ryhmälle tai yksittäiselle käyttäjälle. Rekisteröidyltä on voitu kerätä tapahtuman ilmoittautumisen yhteydessä käytännössä mitä tietoja tahansa, joten jokaisen rekisterin tietosisältö on voinut olla käytännössä mitä tahansa. Tapahtumajärjestäjät kuitenkin tietävät, että tapahtumien ilmoittautujien tiedot näkyvät suurelle joukolle käyttäjiä.

Konsta-palvelussa käytetään käyttäjähallintaan Turun yliopiston identiteetinhallintajärjestelmän käyttäjärooleja. Mikäli yliopiston käyttäjällä on työsuhde yliopistoon, saa hän identiteetinhallintajärjestelmässä myös henkilökunta -roolin. Tämä

roolitieto kulkee käyttäjän kertakirjautumistiedoissa mukana ja näin tietoa saadaan hyödynnettyä myös kertakirjautumista hyödyntävissä palveluissa.3.1 Käyttäjä saattaa olla toisaalta yliopiston henkilökunnan kaltainen työrooliltaan, vaikkei hänellä olisikaan varsinaista työsuhdetta yliopistoon. Tällaisia käyttäjiä ovat esimerkiksi harjoittelijana yliopistolla toimivat henkilöt, tai muut opetus- tai tutkimustyötä yliopistolla tekevät, joilla on tarve päästä henkilökunnan tavoin käyttämään myös yliopiston sähköisiä järjestelmiä ja palveluita. Tällaisista käyttäjistä yliopistolla käytetään nimikettä vierailija. Vierailijasopimuksella tulee olla yliopiston henkilökuntaan kuuluvan käyttäjän puolto.[12] Tällaisille vierailijaksi määritellyille käyttäjille voidaan antaa myös Konsta-järjestelmään henkilökuntaa vastaavat käyttöoikeudet omalla identiteetinhallintajärjestelmän roolilla. Vastaavia rooleja hyödynnetään muutenkin hyvin laajasti Konsta-palvelussa määritettäessä Konstan eri toiminnallisuuksien käyttöoikeuksia. Näin voidaan varmistua palvelun sisällä, että käyttäjällä on täsmälleen oikean laajuiset käyttöoikeudet palvelussa niiden tehtävien hoitamiseen, jotka hänen on Konstaa käyttämällä määrä hoitaa. Kontaktinhallinnan käyttöoikeuksien rajaamisen lisäksi pääsyä palvelussa on rajoitettu esimerkiksi oikeus maksullisten tapahtumien määrittämiseen, kontaktien massatuontiin CSV-tiedoston avulla, viestipohjien luomiseen ja tietysti myös jo edellä mainitut erilaiset roolien käyttöoikeudet.

Rekisterin tietosisällön hallinnointi on haasteellista, kun rekisteröityjä on tuotu erilaisista tietolähteistä ja ovat historian saatossa saattaneet muuttua paljonkin. Rekisteröityjen perustiedot ovat vielä lisäksi luonteeltaan sellaisia, jotka muuttuvat helpolla eikä rekisteri taas toisaalta ole sellainen, johon rekisteröity itse huomaisi muuttuneita tietojaan ilmoittaa. Koska kontaktinhallinta keskitetyn järjestelmän kautta on vielä niin uusi asia Turun yliopistolla, ei palvelun kaikkia toiminnallisuuksiakaan ole vielä ehditty ja toisaalta tehokkaasti myöskään osattu ottaa käyttöön. Konsta -palvelussa on toteutettuna oma käyttöliittymänsä, kontaktiportaali, rekis-

teröityjen käyttöön. Tuon portaalinäkymän kautta rekisteröidyllä on mahdollista päivittää omat tietonsa rekisteriin ja samalla tarkistaa, mitä tietoja hänestä rekisteriin on tallennettu. Koska henkilörekisteri on muodostettu useasta eri lähteestä ja rekisteriin on ollut mahdollista myös itse rekisteröityä, on rekisterissä myös runsaasti duplikaatteja, eli useita kontaktikortteja samasta henkilöstä. Palvelu sisältää omat hallintatyökalut näiden tuplarekisteröityjen hallinnointiin etsien heitä eri yhteystietokenttien perusteella. Kontaktien poistamista ei kuitenkaan tällaisen rekisterin tapauksessa voida automatisoida, joten tuplailmentymien poistaminen vaatii rekisterissä manuaalista työtä. Vastaavasti esimerkiksi kuolleet kontaktit pitää rekisteristä käyttäjien itse poistaa, sillä mikään automatiikka ei tuota rekisterille tietoa menehtyneistä henkilöistä.

Konsta -järjestelmällä ei ole muita ulkoisia liitoksia muihin rekistereihin kuin yllä jo mainittu tietokantatason yhteys Turun yliopiston tietovarastoon. Tietovarasto yliopiston sisäisenä tiedon kokoamisen alustana tuottaa välillisesti Konstaan henkilötietoja opiskelijatietorekisteri Opsusta. Tarkemmin tietovarasto tuottaa rekisteröidyiksi yliopiston valmistuneita tutkinto-opiskelijoita, jotka ovat hyväksyneet liittymisen yliopiston alumniksi. Konsta -järjestelmän kautta oikean roolin omaavilla henkilöillä on mahdollista siirtyä saman kirjautumisen alaisuudessa Emaileri -nimiseen sähköisen markkinoinnin ja uutiskirjeviestinnän palveluun. Konsta -palvelun asetuksiin on tallennettuna tieto käyttäjistä, joille on annettu oikeudet suoraan pääsyyn Emaileri-palveluun Konstan kautta. Konstan henkilörekisteristä käyttäjä voi tehdä haun tai koostaa leikepöytä -toiminnallisuudella joukon rekisteröidyistä ja muodostaa heistä jakelulistan Emaileri -palveluun. Vastaavasti taas Emaileri -palvelun kautta näille rekisteröidyille lähetetyistä viesteistä palautuu merkintä kunkin rekisteröidyn tietoihin. [13]

Konsta henkilörekisterinä on ongelmallinen lähinnä käytön vähäisyyden kannalta. Rekisteröityjen tupla-ilmentymiä ja toisaalta rekisteröityjen yhteystietoja ei re-

kisterissä juurikaan ole korjattu tai päivitetty ja siksi rekisteröityjen tiedot ovat joiltakin osin puutteellisia tai virheellisiä. Tähän liittyen rekisteröidyillä olisi myös mahdollisuus edellä kuvatusti käydä itse tarkastelemassa ja korjaamassa mahdollisesti virheellisesti rekisteriin kirjatut tiedot itsestään erillisen portaali-palvelun kautta, mutta tätä palvelua ei ole Turun yliopistossa otettu vielä virallisesti käyttöön. Rekisteröityjen henkilötietojen näkyvyys on myös liian avoin henkilöstön koulutusrekisteriä hallinnoivien ja kontaktirekisteriä hallinnoivien välillä, vaikka käyttäjämäärän vähäisyyden vuoksi tätä riskiä ei voi pitää merkittävänä. Yksi laajempi ongelma Konsta -kokonaisuuden rekistereissä liittyi tapahtumanhallinnan alla oleviin rekistereihin, eli tapahtumien osallistujalistoihin. Koska koko Turun yliopiston henkilökunnalla oli pääsy tapahtumiin ja niiden osallistujalistoihin, olivat nämä erilliset rekisterit liian avoimen tarkastelun kohteina. Tämän tutkielman tekemisen aikana tähän ongelmaan kehitettiin kuitenkin ratkaisu, jonka myötä jokainen käyttäjä pääsee näkemään palvelussa ainoastaan itse luomansa tapahtumat sekä ne, joihin hänet on merkitty resurssiksi.

3.4 Tietovarasto

Turun yliopiston raportointijärjestelmänä pohjautuu Suomen korkeakoulujen yhteiseen XDW -käsitemalliin, jolloin esimerkiksi sen kautta valtiohallinnolle tehtävä raportointi on lähtökohdiltaan jo yhdenmukaista ja yhdessä sovittua rakennetta noudattavaa. Tietovaraston tietokantarakenne on luotu Turun yliopiston IT-palveluissa. Tietovarasto koostuu tietokantaan yhdistetystä tietosisällöstä, joka on yhdistettyä tietoa eri lähdejärjestelmistä. Toinen merkittävä osa tietovarastoa on näiden tietojen pohjalta koostetut raportit tai raportointiportaalin kautta käytettävät raporttikoosteet. Tietovaraston tietosisältöjen yhdistäminen ja laajat yhteydet eri lähdejärjestelmien tietokantoihin tuottavat pohjaratkaisun monen muun yliopiston järjestelmän toiminnalle, kuten esimerkiksi identiteetinhallintajärjestelmä IDM:n.

Tietovarasto sijaitsee Turun yliopiston omalla virtuaalipalvelinalustalla sijaitsevalla virtuaalipalvelimella. Tietovarastolla on yliopiston sisällä yhteys lähes kaikkiin yliopiston eri tietojärjestelmiin joko suorana tietokantayhteytenä tai mahdollisten siirtotiedostojen tai rajapintatoteutusten kautta. Näin tietovarasto pystyy yhdistämään eri tietolähteistä tulevia aineistoja hyvin laajasti ja koostamaan näin hyvin kattavia raportteja viranomaistarpeisiin, sekä helpottamaan raportteja työssään ja esimerkiksi päätöksenteon tukena tarvitsevia käyttäjiä. Lisäksi öisin siirtotiedostojen kautta tai suoraan lähdejärjestelmän kautta haettu sisältö on tuoretta ja luotettavaa.

Rekisterin tietosisältö koostuu kokonaisuudessaan lähdejärjestelmien tietosisällöistä ja niiden yhdistämisestä. Tietovarasto ei siis toimi varsinaisena lähdejärjestelmänä millekään muulle palvelulle. Tietovarasto sisältää hyvin paljon henkilötietoa eri lähteistä. Erilaisia raportteja varten tietovarastossa käsitellään esimerkiksi henkilöiden palkkatietoja, poissaolotietoja, opintosuorituksia, yliopiston varainhankinnassa kerättyjä lahjoituksia sekä lahjoittajia. Tiedot päivitetään säännöllisesti lähdejärjestelmistä, joten tietosisällön oikeellisuus ja eheys riippuu täysin lähdetiedon oikeellisuudesta ja eheydestä.

Tietovaraston käyttöoikeudet riippuvat aina käsiteltävästä tietoraportista. Itse tietokantakokonaisuuteen käyttöoikeudet ovat lähinnä vain kokonaisuuden ylläpitäjillä, mutta raporttikohtaisesti käyttöoikeudet on mahdollista määritellä Active Directory (AD) käyttäjärekisterin tunnuksiin tai tunnusryhmiin perustuen ja lisäksi esimerkiksi käyttäjän työsopimuksen kustannuspaikkaan, laitokseen tai tiedekuntaan rajoittuvaksi. Lisäksi käyttöoikeusrajoitus voi pohjautua käyttäjän rooliin yliopistolla, eli esimerkiksi henkilökunta, opiskelija tai vierailijasopimukseen perustuva käyttöoikeus. Raporttien sisällä käyttöoikeuksia on vielä mahdollista rajata edelleen tarkemmalle tasolle näkyvyyden osalta. Myös tietovaraston käyttäjähallinta pohjautuu siis Turun yliopiston identiteetinhallintajärjestelmän hallinnoimaan tunnukseen

ja salasanaan, kuten lähes kaikki muutkin sähköiset palvelut yliopistolla.

Tietovaraston ongelmaksi näkisin nimenomaan käyttäjähallinnan ajantasaisuuden, sillä mikään automatiikka ei poista käyttöoikeuksia esimerkiksi henkilön sopimustilanteen tai työtehtävien muuttuessa yliopistolla. Käyttöoikeudet palvelussa rajoittuvat kuitenkin aina tiettyyn raporttiin eivätkä järjestelmäkokonaisuuteen. Lisäksi itse tietovaraston tietokanta on vain hyvin harvojen käyttäjien saavutettavissa. Tietovarasto on kuitenkin tietosisällöltään hyvin laaja ja sen tietosisältö on esimerkiksi tietomurron tapauksessa niin arkaluontoinen, että katson myös käyttäjähallinnan olevan tarpeen olla hallitumpaa palvelussa.

4 Euroopan unionin tietosuoja-asetus

4.1 Tietosuoja-asetuksen käsitteet, vanha direktiivi ja henkilötietolaki

Yhden määritelmän mukaan henkilörekisteri on määritetty olevan "henkilötietoja sisältävää tietojoukkoa, jota käsitellään automaattisen tietojenkäsittelyn avulla, sekä sellaista luetteloa, kortistoa tai muuta näihin verrattavalla tavalla järjestettyä henkilötietoja sisältävää tietojoukkoa, josta tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta"[6] Henkilörekisteri muodostuu siis verrattain helposti minkä tahansa palvelun tai järjestelmän käytön myötä ja tällöin myös rekisteriin päätyneillä henkilöillä on oikeus tietää, mitä tarkoitusta varten he rekisterissä ovat ja kuka pääsee heidän tietojaan siellä käyttämään. Euroopan parlamentti ja Euroopan unionin neuvosto ovat katsoneet, ettei tällaisten henkilörekisterien käyttö vastaa tasapuolisesti eri Euroopan maissa Euroopan parlamentin ja neuvoston 24. lokakuuta 1995 antaman direktiivin 95/46/EY vaatimuksia henkilötietojen käsittelyssä. [14]Tämän vuoksi päätettiin asettaa uusi asetus korjaamaan tätä epätasaisuutta sekä muutoinkin vastaamaan nykyteknologian antamiin mahdollisuuksiin tällaisten rekisterien käsittelyssä. 27. huhtikuuta 2016 asetettiin uusi Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, eli niin kutsuttu

Tietosuoja-asetus, GDPR (General Data Protection Regulation). [3]

Siinä missä vanha direktiivi jätti jäsenvaltioiden itse määrättäväksi ja valvottavaksi suurelta osin henkilörekisterien ja rekisteröityjen henkilösuojan valvonnan[14, 5 artikla], on nyt annettu asetus jo lähtökohdiltaan valvontaan pakottava ja sen lähtökohtana on painottaa enemmän yksilön vapautta ja oikeuksia kuin edeltäjänsä. Uusi tietosuoja-asetus esittelee myös jokusia uusia termejä, joilla täsmennetään huomattavasti melko karkealla tasolla asetettuja asioita edeltäneestä direktiivistä. Vertailtaessa käsitteitä vanhan direktiivin ja nyt annetun asetuksen välillä, iso osa asioita on täysin ennallaan. Henkilötieto määritellään kuten ennenkin olevan luonnolliseen henkilöön liittyvää tietoa, jonka perusteella henkilö on tunnistettavissa. Tällaisia tunnisteita ovat esimerkiksi nimi, henkilötunniste, fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä. Uusina tunnistetietoina asetus tuo kuitenkin määritelmään nykyteknologian mukanaan tuomat verkkotunnistetiedot ja sijaintitiedot. Myöskään henkilötiedon käsittelyn määritelmässä uusi asetus ei poikkea aiemmasta direktiivistä; käsittelyn katsotaan olevan tiedon keräämistä, tallentamista, järjestämistä, säilyttämistä, muokkaamista, hakemista, kyselemistä, käyttöä, luovuttamista, levittämistä, yhdistämistä, poistamista tai tuhoamista. Yhtälailla rekisterinpitäjän määrityksessä ei uusi asetus tuo juuri muutosta aiempaan direktiiviin - pitäjäksi katsotaan edelleen luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu toimielin, joka yksin tai yhdessä toisen kanssa määrittelee henkilötietojen käsittelyn keinot ja tarpeen. Henkilötiedon vastaanottajaksi jo vanha direktiivi määritti luonnollisen tai oikeushenkilön, julkisen viranomaisen, viraston tai muun toimielimen, joka ottaa henkilötietoja vastaan. Tässäkään kohdin uusi tietosuoja-asetus ei tuo muutosta käsitteissä, vaan edelleen vastaanottaja määritellään täsmälleen samalla tavalla. [3, 4 artikla]

Sen sijaan uusi asetus tuo rekisteröidyn, eli henkilörekisteriin kuuluvan henkilön, tietojen jäsentelyyn ja suojaamiseen uudet käsitteet profiloinnin sekä pseudony-

misoinnin. Profiloinnilla asetuksen määrityksen mukaan tarkoitetaan rekisteröidyn käsittelyä, jossa hänen henkilökohtaisten ominaisuuksiensa perusteella hänet analysoidaan tai luokitellaan perustuen hänen terveyteensä, taloudelliseen tilanteeseensa, mieltymyksiin, kiinnostuksen kohteisiin, käyttäytymiseen, sijaintiin tai liikkeisiin. Tämä määritelmätarkennus on seurausta teknologisesta kehityksestä edellisen direktiivin jälkeen - nykyisin henkilöiden luokittelu on huomattavasti helpompaa kuin aiemmin näiden tekijöiden perusteella ja näiden profiilitietojen kerääminen henkilöstä on huomattavasti yksinkertaisempaa. Toinen uusi käsite henkilötietoihin liittyen, pseudonymisointi, taas liittyy henkilötietojen parempaan suojaamiseen henkilörekisterissä. Tämä käsite on yhtälailla seurausta kehittyneestä teknologiasta ja tarkoittaa rekisteröidyn yksilöivien tunnistetietojen säilyttämistä erillisessä rekisterissä erillään varsinaisesta henkilörekisteristä niin, ettei henkilön yksilöinti ole mahdollista ilman teknisiä tai organisatorisia toimenpiteitä.[3, 4 artikla]

Uusi tietosuoja-asetus keskittyy myös entistä tarkemmin tietoturvaloukkauksiin, joita henkilötiedoille voi rekisteristä tapahtua. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jossa rekisterin henkilötietoja tuhotaan vahingossa tai lainvastaisesti, niitä kadotetaan tai luovutetaan luvattomasti tai niihin päästään luvattomasti käsiksi.[3, 4 artikla]

Uusi tietosuoja-asetus tuo siis huomattavasti edeltänyttä direktiiviä paremmin esiin henkilörekisterien käytön valvonnan ja tietoturvan näkökulmat. Siinä missä aiemmin valvonta asetettiin tapahtuvaksi jäsenvaltion säädöksillä ja laeilla[14, 5 artikla], nyt annettu tietosuoja-asetus on määritetty olemaan enemmän kaikkien jäsenvaltioiden noudattama viitekehys, josta edelleen jäsenvaltioiden on mahdollista tehdä yksilöllisiä tarkennuksia ja täsmennyksiä esimerkiksi aloilla, joissa tarvitaan nyt annettua asetusta täsmällisempiä ja yksityiskohtaisempia säännöksiä. Näin on varmistettu, ettei edellisen direktiivin kaltaista jäsenvaltiokohtaista kirjavaa käytäntöä pääse syntymään, kun jo lähtökohdaksi on määritetty tarpeeksi tarkkaan

kuvattu perusta. Lisäksi rekisterinpitäjien ja heitä valvovien tahojen valvonnan vastuutuksella ja jäsenvaltioille yhtenäisillä seuraamuksilla on pyritty tekemään henkilötietojen suojaamisesta enemmän vaatimusta kuin suositusta. Tietosuoja-asetus ottaa lähtökohdaksi myös tekniikan kehittymisen näkökulman tietojen suojeluun; asetuksen mukaan henkilötietojen suojelun ei tulisi olla riippuvainen toteuttavasta tekniikasta eli oltava teknologianeutraalia.

Poikkeuksia tietosuoja-asetus tuo rekisterien käsittelyyn jonkin verran pienten ja keskisuurten, eli alle 250 työntekijän, organisaatioiden osalta[3, 40 artikla]. Kokonaan asetuksen ulkopuolelle on määritetty jäämään kotitalouksien ja yksityisessä käytössä olevien rekisterien henkilötiedot ja niiden käsittely.[3, 2 artikla]

4.2 Periaatteet

Tietosuoja-asetus asettaa henkilötietojen käsittelylle selkeät vaatimukset. Henkilötietojen käsittelyn on oltava lainmukaista, asianmukaista ja rekisteröidyn kannalta läpinäkyvää. Tämä tarkoittaa sitä, että henkilötietojen käsittelyn on tapahduttava laillisten asetusten mukaisesti, ja että henkilötietoja käsitellään kohtuullisesti eli vain välttämättömän määrän. Henkilötietojen turha käsittelyä siis tulisi välttää ja rekisterinpitäjän tulisi pystyä myös osoittamaan tämä käsittelyn tarpeellisuus, eli toiminnan on oltava läpinäkyvää. Henkilötietojen keräämiselle on myös määritettävä selkeä syy, miksi henkilötiedot on kerätty. Lisäksi henkilötietoja ei tulisi käyttää muuhun tarkoitukseen kuin mihin ne on kerätty. Lisäksi rekisteröidystä tulisi kerätä vain se määrä tietoa, mikä on välttämätöntä. Tämä tarkoittaa, ettei rekisteröidystä tulisi säilyttää sellaista tietoa, mitä ei rekisteröinnin syyn vuoksi oikeasti tarvita. Henkilötietojen on oltava myös täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjä velvoitetaan tekemään kaikki mahdolliset kohtuulliset toimenpiteet sen eteen, että rekisteröidystä ei säilytetä virheellistä tietoa, ja että virheelliset ja epätarkat tiedot oikaistaan tai poistetaan viipymättä. Henkilötietoja ei saa myöskään säilyttää

kauempaa kuin mitä tietojenkäsittelyn tarkoitus edellyttää. Tämä tarkoittaa, että kun rekisteröidystä ei ole enää perustetta säilyttää henkilötietoja rekisterissä, tiedot tulisi poistaa. Henkilötietoja tulisi myös päästä käsittelemään vain ne henkilöt, joilla on tarve käsittelyä tehdä. Lisäksi henkilötiedot tulisi säilyttää tavalla, jossa huomioidaan säilyttämisen asianmukainen turvallisuus ja suojaaminen luvattomalta ja lainvastaiselta käytöltä ja vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Ja mikä olennaisinta, rekisterinpitäjän tulee myös osoittaa näiden käsittelyn perusteiden täyttyminen omassa toiminnassaan.[3, 5 artikla]

Nämä vaatimukset ovat selkeä tiukennus edeltäneeseen direktiiviin ja perustuvat nimenomaan siihen lähtökohtaan, että nykyisillä tietoteknisillä keinoilla näiden tietojen asettaminen, seuraaminen ja tarvittaessa siis henkilötietojen poistaminenkin ovat täysin mahdollisia tehdä. Yhtälailla edellytetään nyt uudessa asetuksessa myös tietojen turvaamisen varmistaminen sekä itse tiedon että laitteiston osalta, jolla tietojen käsittelyä tehdään. Rekisterinpitäjää ei velvoiteta hankkimaan lisätietoja henkilöstä, jota rekisteristä ei pystytä tunnistamaan tämän puutteellisten tietojen vuoksi, mutta toisaalta rekisterinpitäjä ei saa myöskään kieltäytyä vastaanottamasta henkilötietoja täydentäviä tietoja, mikäli niitä hänelle tarjotaan.

Henkilötietojen käsittelystä määrätään kuitenkin vielä erikseen asetuksessa, että mikäli rekisterin käyttötarkoitus ei edellytä henkilön tunnistamista, rekisterinpitäjällä ei ole velvollisuutta säilyttää tai hankkia tietoja rekisteröidyn tunnistamiseksi asetuksen vaatimusten täyttämiseksi.[3, 11 artikla]

4.3 Käsittelyn lainmukaisuus

Tietosuoja-asetus määrittää myös periaatteet, joiden mukaan henkilötietojen käsittelyn voidaan katsoa olevan lainmukaista. Näitä oikeusperusteita katsotaan olevan kaikkiaan kuusi: suostumus, sopimus, lakisääteiset velvoitteet, elintärkeiden etujen suojaaminen, yleinen etu sekä oikeutettu etu. [3, 6 artikla]

Mikäli käsittelyn oikeusperuste on suostumus, on tietosuoja-asetuksessa määritetty erityiset ehdot suostumuksen pyytämiselle ja perumiselle. Suostumus tarkoittaa, että rekisteröity on itse antanut suostumuksen henkilötietojen käsittelyyn yhtä tai useampaa käyttötarkoitusta varten. Mikäli käsittelyn perusteeksi katsotaan suostumus, on rekisterinpitäjän pystyttävä myös osoittamaan, että rekisteröity on suostumuksensa antanut. Mikäli suostumus henkilötietojen käsittelylle pyydetään jonkin muun asian yhteydessä, tulee rekisterinpitäjän esittää suostumuksen pyytäminen selkeästi erillään muista asioista ja selkeästi ymmärrettävässä muodossa, selkeällä ja yksinkertaisella kielellä. Annettu suostumus on myös mahdollista perua koska tahansa ja suostumuksen peruuttaminen on oltava yhtä helppoa kuin sen antaminenkin.[3, 7 artikla]

Sopimus käsittelyperusteena tarkoittaa, että henkilötietojen käsittely on edellytys sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on toisena osapuolena. Vastaavasti peruste käsittelylle voi syntyä joidenkin sopimukseen liittyvien toimenpiteiden toteuttamisesta rekisteröidyn pyynnöstä jo ennen kuin sopimus on syntynyt.

Lakisääteiset velvoitteet käsittelyn perusteena tarkoittavat tietysti sitä, että rekisterinpitäjää sitoo jokin lakiin sisällytetty vaatimus tai velvoite, jonka täyttämiseksi rekisterin pitäminen on välttämätöntä. Laki on oltava säädetty joko Euroopan unionin oikeudessa tai jäsenvaltion lainsäädännössä. Vastaavasti yleinen etu käsittelyn perusteena nojautuu organisaation yleisen edun mukaiseen tehtävien suorittamiseen tai julkisen vallan käyttämiseen, joista tavallisimmin säädetään jäsenvaltion laissa tai asetuksessa. Näihin lakiin pohjautuviin käsittelyperusteisiin on asetuksessa jätetty myös jäsenvaltioille vapaus yksityiskohtaisempaan säätämiseen jäsenvaltion omassa lainsäädännössä.

Oikeutettu etu käsittelyn perusteena tarkoittaa, että rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut edellyttävät rekisterin pitämistä ja siinä olevien

henkilöiden henkilötietojen käsittelyä. Mikäli kuitenkin henkilötietojen suojaamista edellyttävät edut rekisteröidylle nousevat näiden rekisterinpitäjän tai kolmannen osapuolen edun ovat olemassa tai rekisteröidyn perusoikeudet tai -vapaudet ovat esteenä rekisterille, ei oikeutettua etua voida käyttää perusteena käsittelylle. Tästä syystä rekisterinpitäjän oikeutettu etu on tavallisesti myös ilmaistava rekisteröidylle, jotta olisi mahdollista arvioida oikeutetun edun vaikuttavuus suhteutettuna rekisteröidyn oikeutettuun etuun.

Elintärkeiden etujen suojaaminen tarkoittaa käytännössä sitä, että jokin rekisteröidyn henkeen kohdistuva asia on riippuvainen rekisterin pitämisestä ja henkilötietojen käsittelystä. Tällaisia voi olla esimerkiksi humanitäärisen avun tarjoamisen vuoksi tai esimerkiksi epidempian leviämisen seuraamiseksi ylläpidettävät rekisterit. [3, 6 artikla]

Vaikka useat rekisterit jäsenvaltioissa täyttäisivätkin nykyisellään uuden tietosuoja-asetuksen asettamat turvallisuuteen ja yksityisyyteen liittyvät vaatimukset, on rekisteröityjen tietoisuudessa rekisteriin kuulumisesta hyvin usein puutteita. Tämän vuoksi tietosuoja-asetuksessa on määritetty entistä tarkemmin se, miten suostumus rekisteriin kuulumisesta tulisi olla annettu ja myös myöhemmin todennettavissa. Suostumus rekisteröidyltä on kerättävä vieläpä niin, että rekisteröidyn on itse tietoisesti merkittävä halunsa rekisteriin kuulumisesta, eikä merkintä saa suostumuksesta kysyttäessä olla edes valmiiksi valittuna. Myös rekisteriin kuulumisen pyynnöstä esitetään asetuksessa tarkentava kuvaus; pyynnön on oltava selkeä ja tiiviisti esitetty eikä rekisteröintipyynnön kohteena olevan palvelun käyttöä häiritsevä.[3, 7 artikla]

Suostumuksen sijaan muiden käsittelyperusteiden käyttäminen on organisaation kannalta huomattavasti helpompi vaihtoehto, mutta tietysti rekisterin luonne ja käyttötarkoitus määräävät hyvin pitkälti sen, mikä käsittelyperuste lopulta on. Tutkimukseni myötä kävi kuitenkin ilmi, että nimenomaan käsittelyperusteen määrit-

täminen rekisterille oli kaikkein eniten tulkinnanvarainen asia rekisterin kannalta juuri tulkinnanvaraisuuden vuoksi. Kun esimerkiksi Suomessa kansallinen laki myöhemmin astuu voimaan, saattaa monen organisaation käsittelyperusteissa tapahtua dramaattisiakin muutoksia, mikäli organisaation tulkinta perusteesta on ollut väärä. Mikäli käsittelyn peruste on jokin muu kuin suostumus, katsotaan ettei rekisteröidyltä tarvitse enää erikseen kysyä suostumusta rekisteriin kuulumisen suhteen. Riittää, kun rekisteröidylle informoidaan kuulumisesta rekisteriin ja henkilötietojen käsittelystä tietosuoja-asetuksen edellyttämällä tavalla.

Luonnolliselle henkilölle tulee ilmoittaa tietojen keruun yhteydessä, miten hänen tietojaan kerätään, mihin tietoja käytetään sekä miten ja missä määrin hänen tietojaan tullaan käsittelemään. Nämä asiat on oltava helposti saatavilla ja ne tulee olla ymmärrettävässä muodossa esitettynä. Henkilötiedon keruun riskit, säännöt, käsittelyn periaatteet, tietosuojatoimet sekä tavat, miten rekisteröity henkilö voi käyttää tietosuojaan liittyviä oikeuksiaan tulee myös ilmoittaa samassa yhteydessä. Vastaavasti, mikäli organisaatio muuttaa esimerkiksi rekisterin käsittelyn perustetta myöhemmässä vaiheessa, tulee siitä informoida rekisteröityjä.[3, 13 artikla]

4.4 Arkaluontoisen henkilötiedon käsittely

Tietosuoja-asetuksessa on erikseen eritelty erityiset henkilötietoryhmät ja erityiset henkilötietotyypit, joiden käsittelyä rekistereissä on erityisesti haluttu kieltää tai ainakin rajoittaa. Tällaista arkaluontoista henkilötietoa ovat rekisteöidyn rotuun, tai etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen tai filosofiseen vakaumukseen littyvät tiedot. Arkaluontoista henkilötietoa on myös rekisteröidyn ammattiliiton jäsenyyteen liittyvät tiedot, geneettisten tai biometristen tietojen käsittely henkilön tunnistamista varten sekä rekisteröidyn terveyttä tai seksuaalista käyttäytymistä tai suuntautumista koskevat tiedot. Lähtökohtaisesti arkaluontoisen henkilötiedon käsittely rekistereissä on kielletty kokonaan. Poikkeuksen tähän voi tuoda

kuitenkin seuraavat erikseen määritellyt seikat. Henkilö itse voi antaa luvan myös arkaluontoisen henkilötiedon käsittelylle rekisterissä, mikäli unionin oikeudessa tai jäsenvaltion lainsäädännössä ei ole säädetty, ettei kieltoa voi suostumuksella kumota. Myös rekisteröidyn tai rekisterinpitäjän velvoitteet tai erityiset oikeudet voivat edellyttää arkaluontoisenkin henkilötiedon käsittelyä rekisterissä työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla. Tällöinkin vain, mikäli unionin oikeus, jäsenvaltion lainsäädäntö tai jäsenvaltion lainsäädännön mukainen työehtosopimus sen sallivat. Laillinen perusta voi tulla myös lainkäyttötehtävien rekistereissä tuomioistuimien toimesta tai yleisen edun nojalla lainsäädäntöön viitaten, mikäli käsittelyn katsotaan olevan oikeasuhteista tavoitteeseen nähden. Käsittely voi olla sallittua myös, mikäli sillä suojataan rekisteröidyn tai toisen luonnollisen henkilön elintärkeitä etuja tai käsittely on tarpeen lainkäyttötehtävissä eri tuomioistuimille. Käsittely voi olla sallittua myös, mikäli rekisteröity on itse asettanut nämä tiedot julkisesti saataville. Käsittelyn salliminen voi muodostua myös poliittisen, uskonnollisen, filosofisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muu yhteisön suorittaman laillisen toiminnan kautta. Myös terveydenhuollon ennaltaehkäisevä työ tai muu asianmukainen rekisteröidyn terveydentilan diagnosointi tai terveydenhuollon hallinnon työ voivat olla perusteena arkaluontoisen henkilötiedon käsittelylle. Tämä kuitenkin edellyttää henkilötietojen käsittelijältä virallista salassapitovelvoitetta. [3, 9 artikla]Myös rikoksen ja rikkomukset on saatettu arkaluontoisena pidettävän henkilötiedon piiriin tietosuoja-asetuksessa, joten näiden tietojen käsittely osana henkilötietoja rekisterissä on yhtälailla kiellettyä asetuksen voimaantulon jälkeen. luonnollisesti viranomaisten valvonnassa pidettävä virallinen rikosrekisteri tekee tähän poikkeuksen, sen pitäminen on edelleen jäsenvaltioissa sallittua.[3, 10 artikla]

4.5 Rekisteröidyn oikeudet

Olennainen osa rekisteröidyn oikeuksia tapahtuu jo siinä vaiheessa, kun henkilötiedot lisätään rekisteriin. On sitten kyse henkilön itsensä rekisteriin tallentamista tiedoista tai jonkun muun tekemästä henkilötietojen rekisteröinnistä, rekisteröidyn tulisi saada tietoonsa muutama perusasia rekisteristä. Osittain rekisteröidylle ilmoitettavat tiedot ovat yhteneviä, ilmoittaa rekisteröity sitten itse henkilötietonsa rekisteriin, tai tiedot saadaan jostakin muusta lähteestä. Nämä kaksi rekisteröimisen tapaa kuitenkin eroavat joiltakin osin merkittävästikin toisistaan rekisteröidyn oikeuksien kannalta ja siksi niiden osalta tiedonantovelvollisuudetkin eroavat hieman toisistaan.

Mikäli henkilötiedot saadaan rekisteröidyltä itseltään, voidaan olettaa henkilön myös tietävän jo lähtökohtaisesti, mitä tietoja hänestä rekisteröidään. Rekisteröidylle pitää kuitenkin kertoa tiedot rekisterinpitäjästä, eli kuka omistaa rekisterin ja keitä toimii omistajan edustajina sekä tarvittavat yhteystiedot rekisterinpitäjään liittyen. Tietosuoja-asetuksessa määritetään myös uusi toimielin organisaatioiden rekistereihin liittyen, tietosuojavastaava. Tietosuojavastaavan tehtävät käsitellään tarkemmin jäljempänä, mutta tietosuojavastaavan ydintehtäviä ovat organisaation rekisterinpitäjien opastaminen ja informointi tietosuoja-asioissa sekä toisaalta seurata, että organisaatio noudattaa rekistereidensä suhteen tietosuoja-asetusta sekä Euroopan unionin ja jäsenvaltion lainsäädäntöjä. Myös tietosuojavastaavan yhteystiedot tulee ilmoittaa rekisteröidylle. Rekisteröidyn tulisi saada tieto rekisterin henkilötietojen käsittelyn oikeusperusteesta sekä oikeutetun edun tapauksessa tarkennusoikeutetusta edusta. Rekisteröidylle on annettava tieto myös henkilötietojen vastaanottajista tai vastaanottajaryhmistä, eli selvennettävä, kuka pääsee henkilötietoja lukemaan. Lisäksi vielä tieto siitä, aiotaanko henkilötietoja siirtää kolmanteen maahan. Ja kuten tietosuojan periaatteet määrittävät, pitää rekisteröidyllä olla tieto henkilötietojen säilytysajasta rekisterissä tai vaihtoehtoisesti säilytysajan määrittä-

misen kriteerit, eli mihin säilytysaika perustuu. Rekisteröidylle pitää myös kertoa hänen oikeuksistaan päästä tarkastamaan rekisteriin tallennetut omat tietonsa sekä oikeudesta pyytää tietojen oikaisemista, poistamista tai käsittelyn rajoittamista sekä vastustaa käsittelyä ja siirtää tiedot järjestelmästä toiseen. Mikäli rekisterin oikeusperuste on suostumus, pitää rekisteröidylle kertoa myös hänen oikeudestaan peruuttaa antamansa suosutumus koska tahansa. Rekisteröidyllä on myös oikeus tehdä valitus rekisterinpitäjästä tai muusta rekisteriin liittyvästä epäkohdasta valvontaviranomaisille, joista myös jäljempänä tarkempi kuvaus. Mikäli käsittelyn oikeusperuste on on lakisääteinen tai sopimukseen perustuva, on rekisteröidylle kerrottava myös, onko henkilötiedot pakko toimittaa, ja mitä tietojen antamatta jättämisestä seuraa. Myös automaattisen käsittelyn avulla tehtävästä rekisteröidyn profiloinnista tulee rekisteröidylle ilmoittaa. Rekisteröidylle on myös kerrottava, mikäli kerättyjä henkilötietoja aiotaan rekisterinpitäjän toimesta käyttää myös muuhun tarkoituksen kuin mitä varten niitä kerätään. Tästä jatkokäsittelystä on kerrottava rekisteröidylle viimeistään ennen jatkokäsittelyä ja ilmoitettava myös tätä käsittelyä koskien säilytysaika sekä oikeudet henkilötietoihin pääsystä, tietojen oikaisemisen ja poistamisen oikeudesta sekä lakiin tai sopimukseen perustuvassa käsittelyssä tiedot henkilötietojen antamatta jättämisen seurauksista.[3, 13 artikla]

Rekisteröidyllä on oikeus pyytää rekisterissä olevia tietojaan. Lisäksi hänellä on oltava oikeus pyytää tietojensa oikaisemista tai poistamista, mikäli tiedot ovat virheelliset tai henkilö haluaa tietojensa poistoa rekisteristä. Rekisteröidyllä on myös oikeus vastustaa tietojensa käsittelyä. Rekisterinpitäjällä on oltava keinot tällaisten pyyntöjen esittämiseen. Pyynnön esittämiseen rekisterinpitäjän tulisi tarjota sähköiset työkalut. Tällaiseen rekisteröidyn esittämään pyyntöön rekisterinpitäjän tulee kyetä vastaamaan ilman viivytystä ja viimeistään kuukauden kuluttua pyynnön esittämisestä. Mikäli pyynnöstä kieltäydytään, tulisi kieltäytyminen pystyä myös perustelemaan. Kieltäytyminen on kuitenkin sallittua, mikäli rekisteröidyllä on jo pyy-

detty tieto, tai tietopyyntöjä on tehty selkeästi niin usein, ettei tietopyynnön pääasiallisena tarkoituksena voida katsoa enää olevan halu saada tietoja haltuun, vaan tuottaa tahallisesti rekisterinpitäjälle erillistä työtä ja vaiva tietojen keräämisestä ja toimittamisesta. Näitä tietopyyntöjä on asetuksen mukaan kuitenkin sallittua tehdä kohtuullisin väliajoin, mutta kuten edellä todettiin, mikäli tieto ei edellisestä tietopyynnöstä ole muuttunut, ei tietoa ole tarvetta toimittaa uudelleen. Tietojen toimittamisesta voidaan kieltäytyä myös silloin, jos tietojen toimittaminen osoittautuu mahdottomaksi tai tuottaa rekisterinpitäjälle kohtuuttomasti työtä. Tietojen luovuttamisen edellytyksenä on, että henkilön henkilöllisyys on kyettävä todentamaan. Rekisterinpitäjän edellytetään käyttävän kaikkia kohtuullisia keinoja henkilöllisyyden todentamiseksi.[3, 15-18 artikla]

Rekisteröidyllä on myös oikeus pyytää tietojensa siirtämistä rekisteristä toiseen, mikäli rekisteröity on itse tietonsa rekisterinpitäjälle antanut. Tiedot on saatava rekisterinpitäjältä yleisesti käytetyssä, koneellisesti luettavassa muodossa, mikäli käsittely rekisterissä on tapahtunut perustuen suostumukseen tai sopimukseen. Siirto rekisteriin tehdään tietystikin vain, jos se on teknisesti mahdollista.[3, 20 artikla]

4.6 Tietojen oikaiseminen ja poistaminen

Rekisterinpitäjällä on velvollisuus ylläpitää rekisterissä oikeellista ja ajantasaista tietoa rekisteröidystä. Vastaavasti rekisteröidyllä on oikeus vaatia rekisterissä olevan puutteellisen tai virheellisen tiedon oikaisemista tai täydentämistä. Oikaisu tai korjaus on tehtävä ilman aiheetonta viivytystä.[3, 16 artikla]

Rekisteröidyllä on oikeus vaatia myös tietojensa poistamista rekisteristä, eli niin kutsuttua unohtamista. Unohtamisen pyytäminen on oikeutettua, jos henkilötietoja ei enää tarvita niihin tarkoituksiin, johon ne alun perin kerättiin tai mikäli rekisteröity peruuttaa antamansa suostumuksen henkilötietojen käsittelyyn ja käsittelyn perustana on ollut suostumus. Rekisteröidyllä on oikeus henkilötietojensa unohta-

misen vaatimiseen, mikäli käsittelyperusteena on ollut oikeutettu etu tai yleinen etu ja rekisteröity on ollut oikeutettu vastustamaan käsittelyä. Myös rekisterinpitäjän henkilötietojen lainvastainen käsittely on peruste rekisteröidylle vaatia tietojensa unohtamista rekisteristä. Unionin oikeus tai jäsenvaltion lainsäädäntö voi edellyttää unohtamista, jotta rekisterinpitäjä saa lakisääteiset velvollisuutensa täytettyä. Unohtaminen itse rekisteristä on yleensä melko helppoa. Haastavaksi rekisteröidyn unohtaminen muodostuu silloin, jos rekisterinpitäjä on julkaissut rekisteröidyn henkilötiedot jollakin tavalla. Tällöinkin rekisterinpitäjän on tehtävä kohtuulliset toimenpiteet saadakseen linkit henkilötietoihin tai mahdolliset jäljennökset tai kopiot poistettua. Kohtuullisuus tässä tapauksessa tarkoittaa käytettävissä olevaa teknologiaa ja toteutumisesta aiheutuvia kustannuksia.[3, 17 artikla]

Rekisterinpitäjän ei tarvitse suorittaa rekisteröidyn unohtamista, mikäli sillä on oikeus tai velvollisuus edelleen rekisteröity rekisterissä säilyttää. Käsittely voi olla edelleen tarpeen sananvapautta tai tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi, tai esimerkiksi rekisterinpitäjän lakisääteisen velvollisuuden täyttämisen vuoksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjän julkisen vallan käyttämistä varten. Myös yleiseen etuun liittyvä arkistointitarkoitus tai tieteellinen tai historiallinen tutkimustarkoitus voi olla peruste unohtamisesta kieltäytymiseen, mikäli unohtaminen hankaloittaisi tätä tarkoitusta huomattavasti.[3, 17 artikla]

Rekisteröidyllä on myös oikeus vaatia henkilötietojensa käsittelyn rajoittamista, mikä tietyt annetut ehdot toteutuvat. Käsittelyä on rajoitettava, mikäli rekisteröity kiistää henkilötietojensa paikkansapitävyyden rekisterissä. Tällöin käsittelyn rajoitusta on rajoitettava siksi aikaa, kunnes rekisterinpitäjä saa varmistettua tietojen paikkansapitävyyden. Käsittelyä on rajoitettava myös, mikäli käsittely on katsottu lainvastaiseksi ja rekisteröity vastustaa henkilötietojensa poistamista ja vaatii käsittelyn rajoittamista sen sijaan. Käsittelyä on rajoitettava myös, mikäli rekis-

terinpitäjä ei enää tarvitse henkilötietoja siihen tarkoitukseen, mitä varten ne on kerätty, mutta rekisteröity sen sijaan tarvitsee tietojaan rekisterissä edelleen oikeudellisen vaateen laatimisen, esittämisen tai puolustamisen vuoksi. Vastaavasti käsittelyä on rajoitettava, mikäli rekisteröity on vastustanut henkilötietojensa oikeutetun tai yleisen edun nojalla suoritettavaa käsittelyä ja ilmaissut rekisteröidyn etujen tulleen aiheetta syrjäytetyksi rekisterinpitäjän etujen vuoksi. Käsittelyn rajoittaminen tarkoittaa käytännössä, ettei henkilötietoja saa käsitellä ilman rekisteröidyn nimenomaista suostumusta rekisterissä. Henkilötietojen säilyttäminen sen sijaan on toki sallittua. Ja vastaavasti rekisteröidylle on ilmoitettava erikseen, kun häntä koskeva käsittelyn rajoitus poistetaan. Rekisterinpitäjän on myös ilmoitettava rekisteröidyn osalta tehdystä oikaisupyynnöstä, unohtamisesta ja käsittelyn rajoittamisesta jokaiselle vastaanottajalle, jolle tietoja rekisteristä on luovutettu, mikäli tämä on kohtuulliseksi katsotuin keinoin mahdollista. Rekisteröidyllä on myös oikeus saada tieto tästä vastaanottajien informoimisesta, mikäli hän sitä pyytää.[3, 18 artikla]

Mikäli henkilötietojen käsittely rekisterissä pohjautuu rekisterinpitäjän yleiseen tai oikeutettuun etuun, on rekisteröidyllä oikeus vastustaa henkilötietojensa käsittelyä. Rekisterinpitäjällä saattaa kuitenkin olla osoittaa perusteet käsittelylle, jotka syrjäyttävät rekisteröidyn edut, oikeudet ja vapaudet, jolloin henkilötietojen käsittely rekisterissä on sittenkin sallittua. Yhtäläisesti rekisteröidyllä on oikeus vastustaa suoramarkkinoinnin tapauksessa henkilötietojensa käsittelyä kyseistä markkinointia varten. Tästä oikeudesta on rekisteröidylle myös ilmoitettava siinä yhteydessä, kun rekisteröityyn ollaan ensimmäistä kertaa yhteydessä.[3, 21 artikla]

4.7 Rekisterinpitäjän vastuut

Tärkein rekisterinpitäjän vastuista on pitää rekisteri turvattuna erilaisten riskien varalta. Riskit voivat olla teknisiä tai käsittelyyn liittyviä. Rekisterinpitäjän oletetaan toteuttavan kaikki tarvittavat toimenpiteet koskien henkilötietojen käsittelyä

koskien niin käsittelytapoja kuin organisatorisiakin toimia sen varmistamiseksi, ettei henkilötietojen tietosuoja vaarannu käsittelyn yhteydessä. Esimerkkinä tietojen suojaamisen hyvistä periaatteista asetus mainitsee henkilötietojen pseudonymisoinnin, joka osaltaan suojaa henkilötietoja nimenomaan käsittelyn myötä tapahtuvien riskien varalta. Toki tekniset ja organisatoriset suojatoimenpiteet ovat yhtälailla olennaisia, sillä tavanomaisesti tietojen käsittelijä on suurin riskitekijä tietosuojan kannalta. Muihin tietoturvaan ja henkilötietojen säilyttämiseen liittyviin riskeihin organisaatio pystyy helpommin varautumaan ja ennakoimaan rikejä, käsittelijän eli ihmisen toimiin ei aina pysty vaikuttamaan. Tämän vuoksi on tärkeää minimoida myös turhaa henkilötietojen käsittelyä ja minimoida henkilöt, joilla on pääsy henkilötietoja käsittelemään. Tästä syystä tietosuoja-asetuksessa määritetään vielä erikseen tietojen käsittelijän vastuita ja velvollisuuksia, jotta rekisterinpitäjien tulisi kiinnitettyä erityisesti huomiota henkilötietojen käsittelijän asianmukaiseen opastukseen ja ohjeistamiseen.[3, 24 artikla]

Mikäli henkilötietoja sisältävä rekisteri sijaitsee jonkin ulkopuolisen toimijan tiloissa ja ylläpidettävänä, kutsutaan tätä ulkopuolista toimijaa henkilötietojen käsittelijäksi. Henkilötietojen käsittelijän on oltava yhtälailla tietoinen henkilötietojen käsittelyn vaatimuksista kuin rekisterinpitäjänkin. Tästä syystä rekisterinpitäjän on oltava tietoinen henkilötietojen käsittelijöistä, eikä käsittelijä näin saa ilman rekisterinpitäjän nimenomaista suostumusta luovuttaa oikeutta henkilötietojen käsittelyyn toiselle käsittelijälle. Asetuksen mukaan henkilötietojen käsittelijän ja rekisterinpitäjän välillä tulisi olla sopimus tai muu laillinen asiakirjaan, jossa käsittelijä sitoutuu oikeelliseen henkilötietojen käsittelyyn. Tässä sitoumuksessa tulisi ilmetä käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. Käsittelijän on käsiteltävä henkilötietoja rekisteripitäjän ohjeiden mukaisesti ja varmistettava, että henkilöt, joilla on oikeus päästä käsittelemään näitä henkilötietoja, ovat sitoutuneet nou-

dattamaan salassapitovelvoitetta. Henkilötietojen käsittelijän velvollisuus on myös auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä täyttämään rekisteröidyn oikeuksiin kuuluvien tietopyyntöjen koostamisen ja toimittamisen. Kun käsittelyyn liittyvät palvelut päättyvät, on käsittelijä myös velvollinen palauttamaan rekisterinpitäjälle kaikki käsittelyn alaisena olleet henkilötiedot ja poistamaan olemassa olevat jäljennökset. Käsittelijän velvollisuus on myös saattaa rekisterinpitäjän saataville kaikki tarvittavat tiedot, jotta rekisterinpitäjä voisi täyttää tietosuoja-asetuksessa hänelle asetetut vaatimukset ja velvollisuudet.[3, 28 artikla]

4.7.1 Tietosuojailmoitus - Seloste käsittelytoimista

Jokaisen rekisterinpitäjän tulee ylläpitää selostetta vastuullaan olevista käsittelytoimista. Selosteesta on käytävä ilmi rekisterinpitäjän, rekisterinpitäjän edustajan ja mahdollisen tietosuojavastaavan yhteystiedot. Lisäksi rekisterin käsittelyn tarkoitukset on kuvattava sekä tieto henkilötietojen vastaanottajista, joille henkilötietoja on luovutettu tai luovutetaan. Tarvittaessa myös tieto henkilötietojen siirrosta kolmansiin maihin. Mikäli mahdollista, olisi selosteessa kuvattava myös eri henkilötietoryhmien poistamisen suunnitellut määräajat. Lisäksi olisi hyvä kuvata tekniset ja organisatoriset turvatoimet henkilötietojen suojaamiseksi niiltä osin kuin mahdollista.[3, 30 artikla]

Myös henkilötietojen käsittelijän tulee ylläpitää selostetta käsittelytoimista. Selosteesta tulee käydä ilmi henkilötietojen käsittelijän sekä kunkin rekisterinpitäjän, jonka rekistereiden henkilötietoja käsitellään tai mahdollisen henkilötietojen käsittelijän edustajan tai tietosuojavastaavan yhteystiedot. Vastaavasti käsittelijän selosteesta tulisi käydä ilmi mahdollinen henkilötietojen siirto kolmansiin maihin sekä mahdollisuuksien mukaan organisatoriset ja tekniset turvatoimet, joilla rekistereitä ja niissä olevia henkilötietoja turvataan. Tämä selosteen laatimisen velvollisuus

on yhtälailla kuitenkin rajattu koskemaan vain yli 250 työntekijän organisaatioita, kuten rekisterinpitäjänkin osalta asetuksessa on tehty.[3, 30 artikla]

4.8 Henkilötietojen tietoturva

Jo edellä kuvattiin yleisellä tasolla tietosuoja-asetuksen edellyttämiä organisatorisia ja teknisiä ratkaisuja, joita rekisterinpitäjältä tietosuojan varmistamiseksi edellytetään. Tällaisia voivat olla esimerkiksi henkilötietojen pseudonymisointi ja salaus tai palveluiden luottamuksellisuuden ja eheyden sekä käytettävyyden ja vikasietoisuuden varmistaminen. Rekisterinpitäjän tulisi arvioida henkilörekisterin tietoturvan taso ja kiinnittää arviossaan erityistä huomiota nimenomaan riskeihin, joita henkilötietojen käsittely sisältää ja toisaalta, joita henkilötietojen tallentaminen sisältää. Näihin liittyen riskejä on esimerkiksi tietojen häviämisen, muuttamisen, luvattoman luovuttamisen tai luvattoman henkilötietoihin pääsyn näkökulmasta olemassa. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että rekisteröityjen henkilötietoja käsittelevät henkilöt toimivat käsittelyssään rekisterinpitäjän ohjeiden mukaisesti.[3, 32 artikla]

Tietosuoja-asetuksessa on määritetty myös selkeät toimenpidevaatimukset ja aikarajat tilanteiden varalle, jossa henkilörekisterin tietoturvaa on tavalla tai toisella rikottu. Ensisijainen tehtävä rekisterinpitäjällä on ilmoittaa sekä valvontaviranomaisille että rekisteröidylle tapahtuneesta tietoturvaloukkauksesta. Viranomaisille ilmoitus on tehtävä viimeistään 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta. Tämä kuitenkin vain silloin, mikäli tietoturvaloukkaus aiheuttaisi todennäköisesti rekisterissä olevan luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvan riskin. Ilmoituksessa on toimitettava kuvaus tapahtuneesta tietoturvaloukkauksesta, sekä mahdollisuuksien mukaan rekisteröityjen ryhmät ja määrät sekä henkilötietotyyppien ryhmät ja lukumäärät. Valvontaviranomaiselle on toimitettava ilmoituksessa myös tietosuojavastaavan nimi ja yhteystiedot, sekä tietoturvaloukkauksen ai-

heuttamat todennäköiset seuraukset. Lisäksi viranomaiselle on toimitettava tiedot ehdotetuista tai toteutetuista toimenpiteistä, joita rekisterinpitäjä on tapahtuneen loukkauksen johdosta tehnyt. Mikäli ilmoitusta ei tehdä 72 tunnin kuluessa, on rekisterinpitäjän toimitettava valvontaviranomaiselle selvitys tapahtuneesta. Rekisterinpitäjän on dokumentoitava tarvittavassa laajuudessa kaikki tapahtuneet tietoturvaloukkaukset ja niiden vaikutukset sekä niiden aiheuttamat korjaavat toimenpiteet Tämän dokumentaation avulla valvontaviranomaisen on pystyttävä tarvittaessa tarkistamaan, että tietosuoja-asetusta on tältä osin noudatettu. Yhtäläisesti henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle ilmi tulleesta tietoturvaloukkauksesta viipymättä.[3, 33 artikla]

Rekisteröidylle rekisterinpitäjän on ilmoitettava tapahtuneesta tietoturvaloukkauksesta ilman aiheetonta viivytystä, mikäli se todennäköisesti aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille. Rekisteröidylle on ilmoitettava samat yksityiskohdat tapahtuneesta tietoturvaloukkauksesta kuin valvontaviranomaisellekin. Asetus määrittää kuitenkin erotuksena valvontaviranomaiselle toimitettavaan ilmoitukseen, että rekisteröidylle toimitettava ilmoitus on tehtävä selkeällä ja yksinkertaisella kielellä. On kuitenkin muutama poikkeustilanne, jossa ilmoitusta rekisteröidylle ei vaadita. Mikäli rekisterille on toteutettu sellaiset suojatoimenpiteet, joiden myötä sen henkilötiedot eivät ole ymmärrettävissä muiden kuin rekisteriin oikeellisesti pääsevien, kuten esimerkiksi rekisterin tietojen salaaminen, on katsottavissa, ettei tapahtuneesta tietoturvaloukkauksesta ole tarpeen ilmoittaa rekisteröidylle. Myös silloin rekisteröidylle ei katsota olevan tarpeen ilmoittaa, mikäli tietoturvaloukkauksen jälkeen rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joiden myötä tapahtunut tietoturvaloukkaus ei todennäköisesti enää tapahdu. Kolmas poikkeustapaus, jolloin rekisteröidylle ei ole tarpeen ilmoittaa tapahtuneesta tietoturvaloukkauksesta on, mikäli ilmoittamisesta koituisi kohtuuttomasti vaivaa. Tällöin kuitenkin rekisterinpitäjä on velvoitettu tekemään julkisen tiedonannon tai vastaavan toimenpiteen,

jolla rekisteröidylle tiedotetaan yhtä tehokkaalla tavalla. Myös valvontaviranomainen voi tehdä päätöksen ilmoituksen tarpeellisuudesta rekisteröidylle, mikäli rekisterinpitäjä ei ole itse ilmoitusta vielä tehnyt.[3, 34 artikla]

4.9 Tietosuojavastaava

Rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava esimerkiksi kun henkilötietojen käsittelyä tekee jokin julkishallinnon elin, joka ei kuitenkaan ole tuomioistuin. Myös laajamittaisen rekisteröityjen säännöllisen ja järjestelmällisen seurannan ollessa rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävää, on tietosuojavastaavan nimittäminen pakollista kuin myös ydintehtävien koskiessa erityisiä henkilötietoryhmiä koskevaan laajamittaiseen käsittelyyn. Pääsääntöisesti organisaatiolle riittää yksi tietosuojavastaava. Rekisterinpitäjän tai henkilötietojen käsittelijän on julkaistava sekä ilmoitettava valvontaviranomaisille tietosuojavastaavan yhteystiedot.[3, 37 artikla]

Tietosuojavastaavan on syytä olla osallisena henkilötietojen suojaa koskevien asioiden selvittelyssä ja suunnittelussa riittävän ajoissa ja tarvittavassa laajuudessa. Tietosuojavastaavan tekemää työtä organisaatiossa on tuettava tarjoamalla tälle tarvittavat resurssit ja pääsy tarvittaviin tietoihin ja rekistereihin työn suorittamiseksi. Työssään tietosuojavastaavan on toimittava itsenäisesti noudattaen vain tietosuojasta asetettuja lakeja ja asetuksia eikä hän saa työssään olla vaikutuksen alaisena rekisterinpitäjän tai henkilötietojen käsittelijän tai muun organisaation toimielimen vaikutukselle. Tietosuojavastaava voi suorittaa organisaatiossa myös muita työtehtäviä ja velvollisuuksia, kunhan nämä eivät ole eturistiriidassa tietosuojavastaavan tehtävien kanssa. Tietosuojatyönsä suorittamisesta tietosuojavastaavaa ei saa myöskään rangaista tai erottaa sen vuoksi, että hän on hoitanut oman työnsä. Raportoinnin tietosuojavastaava tekee suoraan rekisterinpitäjän tai tietojen käsittelijän ylimmälle johdolle. Tietosuojavastaava on vaitiolovelvollinen suorittamastaan

työstä.[3, 38 artikla]

Tietosuojavastaavan tehtäviin kuuluu antaa organisaatiossa neuvoja ja tietoja tietosuoja-asetuksen ja tietosuojasäännösten mukaisista velvollisuuksista. Tietosuojavastaava myös seuraa aktiivisesti, että organisaation eri rekisteripitäjät tai henkilötietojen käsittelijät noudattavat tietosuojalainsäännöksiä ja toimivat oikein tietosuojaan liittyvissä asioissa, kuten esimerkiksi vastuunjaossa, tiedon lisäämisessä, henkilöstön kouluttamisessa sekä tarkastuksissa. Tietosuojavastaavan olennainen tehtävä on myös tehdä yhteistyötä valvontaviranomaisten kanssa sekä toimia valvontaviranomaisen yhteyspisteenä organisaatioon ja sen tietosuoja-asioihin liittyen. [3, 39 artikla]

4.10 Valvontaviranomaiset

Jokaisen Euroopan unionin jäsenvaltion on varmistettava, että yski tai useampi riippumaton valvontaviranomainen valvoo tietosuoja-asetuksen soveltamista jäsenvaltiossa niin, että henkilöiden perusoikeudet ja -vapaudet tulevat suojatuiksi. Valvontaviranomaisten tulee tehdä yhteistyötä, jotta voidaan taata asetuksen yhdenmukainen soveltaminen koko unionin alueella. Valvontaviranomaisen riippumattomuuden varmistamiseksi, hän ei saa ottaa vastaan ohjeita, eikä olla minkään ulkopuolisen vaikutuksen alainen, jotta mikään taho ei pääse vaikuttamaan hänen oikeudenmukaiseen tehtäväänsä asetuksen noudattamiseksi. Valvontaviranomainen ei saa tehtävänsä ohessa myöskään harjoittaa ammattitoimintaa tai tehtäviä, jotka olisivat ristiriidassa hänen toimiessaan valvontaviranomaisen roolissaan. Jäsenvaltion on taattava valvontaviranomaiselle tarvittavat resurssit ja henkilöstö tehtävän suorittamiseksi. Valvontaviranomaisen on oltava taloudellisesti valvottu taho, jolla on oma vuotuinen talousarvionsa, joka voi olla osa valtion tai kansallista talousarviota.[3, 51 artikla]

Valvontaviranomaisten jäsenet tulee nimetä jäsenvaltiossa läpinäkyvästi ja nimit-

täjä tulee toimia jäsenvaltion parlamentti, hallitus, valtionpäämies tai jäsenvaltion laissa nimittämiseen määrätty riippumaton elin. Jäsenet nimitetään toimikaudeksi ja jäsenen tehtävät päättyvät vasta toimikauden päättyessä tai jäsenen jäädessä pakolliselle eläkkeelle jäsenvaltion lainsäädännön mukaisesti. Jäsen voidaan erottaa ainoastaan vakavan väärinkäytöksen perusteella tai jos hän ei enää täytä tehtävän suorittamiseen tarvittavia edellytyksiä. Kunkin unionin jäsenvaltion tulee säätää laissaan valvontaviranomaisen perustamisesta, jäseneksi nimitettävän pätevyysvaatimuksista ja kelpoisuusehdoista, jäsenten toimikauden kestosta sekä uudelleennimittämisen mahdollisuudesta. Kaikkia valvontaviranomaisen jäseniä koskee vaitiolovelvollisuus toimeensa liittyviin asioihin sekä toimikautensa aikana, että sen jälkeen.[3, 52 artikla]

Valvontaviranomaisen tehtäviin kuuluu valvoa tietosuoja-asetuksen soveltamista ja panna täytäntöön se alueellaan. Hänen on edistettävä alueellaan yleistä tietoisuutta ja ymmärrystä henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. Lisäksi valvontaviranomaisen tulee toimia neuvonantajana kansallisten lainsäädännöllisten ja hallinnollisten toimenpiteiden asettamisessa koskien luonnollisen henkilön oikeuksien ja vapauksien suojelua. Valvontaviranomaisen tulee toimia kansallisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden tietämystä kasvattavana tahona sekä antaa rekisteröidyille pyydettäessä tietoa tietosuoja-asetuksen mukaisten oikeuksien käytöstä. Valvontaviranomainen myös käsittelee rekisteröityjen tai muiden tahojen tekemiä valituksia ja tutkii valituksen kohteena olleita tapauksia sekä pitää valituksen tehneen tahon tietoisena tutkinnan etenemisestä ja tuloksista. Valvontaviranomainen toimii kansallisella taholla myös hyväksyjänä, laatijana ja neuvonantajana useissa tietosuoja-asetukseen liittyvissä lausekkeissa, luetteloinneissa ja säännöissä, joilla määritetään jäsenvaltiotasolla määritettäviä perusteita kansallisista toimista liittyen tietosuojaan. Valvontaviranomaisella on valta määrätä jäsenvaltion alueella rekisterinpitä-

jien ja henkilötietojen käsittelijöiden luovuttamaan ja mahdollistamaan pääsy tarvittaviin henkilötietoihin, jotta valvontaviranomaisen olisi mahdollista suorittaa tehtäväänsä. Lisäksi valvontaviranomaisen tulee ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle väitetystä tai havaitusta rikkomuksesta sekä hänellä on valta toteuttaa tutkimusta tietosuojaan liittyvissä tarkastuksissa. Luonnollisesti valvontaviranomaisella on toimivalta tehdä varoituksia ja huomautuksia rekisterinpitäjän tai henkilötietojen käsittelijän käsittelytoimien säännösten vastaisuudesta jo etukäteen. Valvontaviranomaisella on myös toimivalta määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, mikäli pyyntö on tietosuoja-asetuksen mukaisesti aiheellinen. Valvontaviranomainen saa myös määrätä tietosuoja-asetuksen vastaisten käsittelytoimien korjaamisesta, tietoturvaloukkauksen ilmoitusvelvollisuuden täytäntöönpanosta sekä käsittelyn rajoittamisesta, käsittelykiellosta, tietojen oikaisusta tai poistamisesta sekä määrätä sakkoja tietosuojaan liittyvistä rikkeistä tietosuoja-asetuksen mukaisesti. Lisäksi valvontaviranomaisen tulee laatia vuosittain toimintakertomus, johon voi sisältyä luettelo ilmoitettujen rikkomusten ja toteutettujen toimenpiteiden tyypeistä. Nämä kertomukset tulee toimittaa kansalliselle parlamentille, hallitukselle ja muille kansallisessa lainsäädännössä nimetyille viranomaisille sekä saatettava yleisön, komission ja tietosuojaneuvoston saataville.[3, 57 artikla]

4.11 Oikeussuojakeinot, vastuu ja seuraamukset

Jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos rekisteröity katsoo, että häntä koskevien tietojen käsittelyssä rikotaan tietosuoja-asetusta. Valvontaviranomainen ilmoittaa ilmoituksen tekijälle, miten tämän tekemä valitus etenee ja mikä sen ratkaisuksi on tullut. Mikäli valvontaviranomainen ei ole käsitellyt rekisteröidyn tekemää valitusta tai ilmoittanut kolmen kuukauden kuluessa valituksesta tietoja sen etenemisestä, on rekisteröidyllä oikeus tehokkaisiin oikeus-

suojakeinoihin. Mikäli henkilölle aiheutuu tietosuoja-asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, on hän oikeutettu saamaan korvauksen aiheutuneesta vahingosta rekisterinpitäjältä tai henkilötietojen käsittelijältä. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta, joka asetusta rikkovasta käsittelystä on aiheutunut.

Henkilötietojen käsittelijä taas on vastuussa asetuksen rikkomisesta, mikäli on toiminut käsittelijälle asetuksessa määritettyjen toimintatapojen vastaisesti, tai on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen vastaisesti. Mikäli tietosuoja-asetuksen rikkomisen luonne ja vakavuus, rikkeen tahallisuus tai tuottamuksellisuus sekä esimerkiksi niiden rekisteröityjen lukumäärä, joihin rikkomus vaikuttaa ovat merkittäviä, voi rikkomuksesta seurata jopa sakkorangaistus. Rikkomusta voivat lieventää toimenpiteet, joita rikkeen jälkeen on tehty asian kuntoon saattamiseksi. Vastaavasti taas rikkomuksen voidaan katsoa olevan vakavampi, jos saman rekisterinpitäjän tai henkilötietojen käsittelijän taustalla on useampia vastaavia rikkomuksia, tai jos rikkominen on toistuvaa. Myös yhteistyöhalukkuus valvontaviranomaisten kanssa voidaan katsoa lieventäväksi tekijäksi rikkomukselle. Sakkorangaistus rekisterinpitäjälle tai henkilötietojen käsittelijälle on tietosuoja-asetuksessa määritetty olevan 10000000 tai 20000000 euroa, riippuen rikotusta asetuksen artiklasta. Tai jos kyseessä on yritys, kaksi tai neljä prosenttia sen edellisen tilikauden vuotuisesta kokonaisliikevaihdosta, mikäli osuus liikevaihdosta ylittää edellä mainitut rahasummat.

4.12 Yhteenveto organisaation ja rekisterinpitäjän velvollisuuksista

Organisaation tulee jokaisen sen omistaman henkilörekisterin osalta täyttää Tietosuoja-asetuksen perusvaatimukset henkilötietojen säilyttämiselle sisäänrakennetusti ja ole-

tusarvoisesti. Suomessa tietosuojalainsäädännön ja Tietosuoja-asetuksen noudattamista valvoo kansallisesti Tietosuojavaltuutetun toimisto. Tietosuojavaltuutetun toimisto koostuu Tietosuojavaltuutetusta, kahdesta apulaistietosuojavaltuutetusta sekä 40 hengen joukosta asiantuntijoita (9.6.2022) [15]. Tietosuojavaltuutetun toimisto on antanut listan Tietosuoja-asetuksessa määritetyistä tietosuojaperiaatteista, joita organisaation tulisi noudattaa täyttääkseen Tietosuoja-asetuksen asettamat vaatimukset [16]. Tietosuojaperiaatteiden mukaan henkilötietoja on

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten
- käsiteltävä luottamuksellisesti ja turvallisesti

Yllä esitettyyn listaan kiteytyy Tietosuoja-asetuksen vaatimukset ja velvollisuudet organisaatiolle. Näitä vaatimuksia olen kutakin käsitellyt tarkemmin tässä luvussa aiemmin. Jokainen listan kohta on yhtälailla merkittävä eikä velvollisuuksia voi asettaa tärkeys- tai muuhunkaan järjestykseen. Tietosuojaperiaatteita on noudatettava koko henkilötietojen käsittelyn elinkaaren ajan. Mikäli organisaatio pystyy täyttämään nämä periaatteet henkilötietojen käsittelyssä omistamansa henkilörekisterin osalta, voidaan sanoa sen olevan kyseisen rekisterin osalta tietosuoja-asetuksen mukainen. Vastaavasti, mikäli organisaatio pystyy kaikkien henkilörekisteriensä osalta

täyttämään tietosuojaperiaatteet, voidaan katsoa koko organisaation toimivan ja käsittelevän hallinnoimiaan henkilötietoja Tietosuoja-asetuksen mukaisesti.

5 Tietosuoja-asetuksen vaikutukset Turun yliopistossa

5.1 Opiskelijarekisteri

Turun yliopiston opiskelijarekisteri on tätä työtä kirjoittaessa murrosvaiheessa, sillä vuosia käytössä ollut vanha järjestelmä ollaan korvaamassa uudella. Opiskelijarekisteri on yliopistolle tietyllä tavalla hyvin selkeä henkilörekisterinä, sillä sen olemassaolo on laissa määrätty ja sen varaan rakentuu yksi yliopiston myöskin laissa määrätty ydintehtävä, opetuksen järjestäminen. Tämä kahden eri järjestelmän murrosvaihe asettaa kuitenkin oman haasteensa kummallekin järjestelmälle, sillä samaan aikaan, kun toista ollaan ottamassa käyttöön ja toista lopettamassa, tulisi tietosuoja-asiat huomioida kummankin rekisterin osalta. Koska lopetettava opiskelijarekisteri on ikänsä ja vanhan teknologiansa vuoksi haastavampi tietosuojan näkökulmasta, keskityn tutkimuksessani käsittelemään näistä rekistereistä ainoastaan sitä.

5.1.1 Palvelun tietoturvallisuus

Turun yliopiston opiskelijarekisteri sijaitsee yliopiston omassa konesaliympäristössä sijaitsevalla virtuaalipalvelinalustalla. Turun yliopistolla on oma tietoturvapolitiikka, johon kaikki yliopiston ylläpitämät henkilörekisterit nojaavat ja jonka mukaan

sen tarjoamat palvelut tuotetaan.[17] Sen mukaisesti kaikki opiskelijarekisterinkin käyttäjät noudattavat yliopiston käyttösääntöjä käsitellessään henkilötietoja rekisterissä. Sen mukaan jokainen yliopiston käyttäjä on velvoitettu toimimaan säädettyjen lakien ja asetusten mukaan toimiessaan yliopiston myöntämällä käyttäjätunnuksella sekä velvoitetaan vaitiolovelvollisuuteen saamistaan salassapidettävistä tiedoista. [18] Palvelua on mahdollista ylläpitää vain yliopiston verkkolokaatioon kytketyltä työasemalta tai erillisen VPN-toteutuksen (Virtual Private Network) kautta. Palvelun käyttö vaatii aina kirjautumisen yliopiston myöntämällä verkkotunnuksella. Näiden seikkojen myötä voidaan sanoa, että organisaation taholta palvelun tietoturvallisuus on pyritty takaamaan niin kuin se teknisesti on mahdollista.

5.1.2 Opsu ja rekisterinpitäjän velvollisuudet

Opiskelijarekisteriin kerätään kaikkien Turun yliopiston opiskelijoiden perustiedot sekä tiedot erilaisista opintosuorituksista ja muista opiskeluun liittyvistä tiedoista, kuten läsnäolotiedot, ilmoittautumiset yms. Rekisteri ei sisällä niinkään arkaluontoiseksi luokiteltavaa henkilötietoa, mutta rekisterissä säilytettävät henkilötiedot voisivat esimerkiksi päätyessään tietomurron myötä asiattomien tajojen käsiin aiheuttaa vakavaa vahinkoa rekisteriin kuuluville. Tästä syystä niiden turvallisesta säilyttämisestä on huolehdittava asianmukaisesti. Opiskelijarekisterin henkilötietojen käsittelyn oikeusperustana on katsottu olevan yleinen etu. Opiskelijarekisteri on ensisijaisesti olemassa, jotta yliopistossa voitaisiin tehokkaasti hoitaa yhtä yliopistolaissa määritettyä perustehtävää, opetusta. [9]

Opiskelijarekisterissä henkilötietojen käsittelyltä ei oikeastaan voida välttyä, sillä opiskelijan henkilötietoihin on päästävä käsiksi esimerkiksi merkittäessä hänelle opintosuoritusta, hyväksyttäessä hänet kurssille tai tehtäessä muita vastaavia opetuksen järjestämiseen liittyviä tehtäviä, joiden vuoksi koko rekisteri on olemassa. Näin opiskelijarekisterin suhteen merkittävin huolehdittava asia onkin varmistaa,

että henkilötietoihin on pääsy vain niillä henkilöillä, joilla on työtehtäviensä vuoksi tarve niihin päästä käsiksi. Opsussa käyttöoikeuksia anotaan erillisellä lomakkeella, jossa tarve perustellaan, ja jonka pohjalta palvelun pääkäyttäjät arvioivat käyttöoikeuksien myöntämisen perusteet joko riittäviksi tai riittämättömiksi. Tutkimusta varten haastatteluja tehdessäni kävi kuitenkin ilmi, että käyttöoikeuksien poistuminen ei ole palvelussa millään tavalla automatisoitu, eli henkilön työtehtävien muuttuessa tai loppuessa palvelun käyttöoikeudet eivät automaattisesti katkea. Opiskelijarekisterin kanssa työskentelevän henkilön käyttäjätunnus yliopistolle saattaa nimittäin jatkua siitä huolimatta, että hänen työsopimuksensa yliopistolla päättyy siitä syystä, että hänellä saattaa olla opiskeluoikeus yliopistossa tai avoimessa yliopistossa. Näiden käyttäjät toimivat yliopistossa aivan vastaavilla käyttäjätunnuksilla, eikä pelkästä käyttäjätunnuksesta voida päätellä, missä roolissa käyttäjä yliopistolla toimii. Tätä epäkohtaa ja sen korjaamista varten kehitimme yhdessä palvelun pääkäyttäjän sekä yliopiston IT-palveluiden asiantuntijan kanssa raporttiajon, jolla muuttuneiden käyttäjätunnusten valvominen on mahdollista. Yliopiston tietovarasto pystyy tarkkailemaan sekä opiskelijarekisterin käyttöoikeuksia, että yliopiston käyttäjien sopimuksia, olivatpa ne työsopimuksia tai opiskeluoikeuteen liittyviä. Mikäli tietovarastoon luodussa taulussa havaitaan poikkeus, eli muutos opiskelijarekisteriin käyttöoikeudet omaavan henkilön sopimustilanteessa, saa pääkäyttäjä siitä ilmoituksen sähköpostiinsa ja voi arvioida uudelleen tarpeen rekisteriin pääsylle. Toinen merkittävä rekisteröityjen tietoihin pääsyyn liittyvä tietosuojahaavoittuvuus liityi opiskelijarekisterin edeltäneeseen sovellusversioon, joka havaittiin edelleen olevan asennettuna useiden rekisteriä käyttäneiden työasemilla. Koska sovelluksesta asennettua versiota ei ollut tietoturvan näkökulmasta tarkasteltu, saati sitten päivitetty vuosiin, oli käsillä suuri riski tietosuojaloukkaukselle. Sen poistamiseksi varmistettiin ensin, että tarvittava tieto rekisteröidyistä oli otettu rekisteristä talteen, minkä jälkeen rekisteristä työasemilla olleet versiot poistettiin hallitusti Turun yliopiston

IT-tuen asiantuntijan toimesta.

Opiskelijarekisterin suhteen kaikkia tietosuoja-asetuksen vaatimuksia ei pystytty kohtuullisen työmäärän puitteissa toteuttamaan. Palvelu kerää lokimerkintöjä palvelun käytöstä, kirjautumisesta palveluun ja tehdyistä muutoksista, mutta henkilötietojen käsittelystä pelkästään tietojen lukemisen eli henkilötietojen käsittelyn osalta ei synny lokiin merkintöjä. Palvelun ollessa kuitenkin elinkaarensa loppupäässä todettiin, että tämän toiminnallisuuden toteuttaminen rekisteriin olisi vaatinut kuitenkin kohtuuttoman työmäärän. Sen sijaan Turun yliopistossa päädyttiin varmistamaan muilla tavoin tietosuojan vaatimusten mukainen käyttö ja toteuttaa tulevaan opisjkelijarekisteriin paremmin tietosuoja-asetuksen ehdot täyttävät ominaisuudet. Tietosuoja-asetuksen vaatimuksen mukaisesti opiskelijoista on tähän rekisterin tallennettuna vain oleellinen tieto. Rekisterin tarkoituksena on olla opiskelijalle sekä Turun yliopistolle työvälinen opiskelijan opintojen edistymisen seurantaan sekä taata kummankin osapuolen oikeusturva opiskelijan opintosuoritusten suhteen. Tästä syystä koko rekisteri on rakennettu lähtökohtaisesti jo täyttämään juuri ne minimivaatimukset, mitä oikeusturvan varmistaminen vaatii, koska koko rekisterin olemassaolo perustuu lain asettamiin vaatimuksiin. Rekisterissä olevat henkilötiedot saadaan pääosin opiskelijalta itseltään henkilön hakiessa opiskelijaksi Turun yliopistoon. Henkilö luodaan rekisteriin siinä vaiheessa, kun hänet hyväksytään opiskelijaksi. Henkilötietojen päivittämisen pystyy opiskelija itse tekemään saman käyttöliittymän kautta, jossa hänen opintosuorituksensa sijaitsevat. Henkilötietoja rekisteriin ei päivitetä keskitetysti minkään ulkoisen palvelun kautta, vaan opiskelija velvoitetaan pävittämään muuttuneet tietonsa itse saadakseen esimerkiksi yliopiston postitse lähettämiä kirjeitä tai muita postituksia itselleen. Tästä syystä rekisterissä olevia henkilötietoja ei pääsääntöisesti päivitetä automaattisesti. Tarjoamalla käyttöliittymän omien tietojensa päivittämiseen opiskelijalle, on rekisterinpitäjä huolehtinut mahdollisuudesta päästä itse ylläpitämään tietojaan ja huolehtinut tietojen

ajantasaisuudesta rekisterissä. Mutta vain osittain. Koska osa opiskelijarekisterin tiedoista on arkistolaissa määrätty säilytettäväksi pysyvästi, on rekisterinpitäjän säilytettävä myös rekisteröidyt henkilöt rekisterissä. Koska tietosuoja-asetus vaatii rekisterinpitäjää ylläpitämään rekisteröityjen henkilöiden henkilötietoja ajantasaisina, poistetaan rekisteristä ei-aktiivisten henkilöiden tiedot niiltä osin kuin tietojen vanheneminen on todennäköistä, koska opinto-oikeuden päätyttyä opiskelija ei voi enää käyttää tarjottua käyttöliittymää tietojensa päivittämiseen. Tällaisia rekisteristä ei-aktiivisilta käyttäjiltä poistettavia tietoja ovat esimerkiksi henkilön osoite-, sähköpostiosoite sekä puhelinnnumerotiedot. Koska rekisterin luonne on edellä esitetysti yliopiston kannalta sellainen, että rekisteröityjen tietojen säilyttäminen on yliopiston arkistointivelvoitteiden alainen, ei rekisteröidyllä ole myöskään oikeutta pyytää itsensä unohtamista rekisteristä.

Opiskelijarekisteriin käyttöoikeudet omaa laaja joukko käyttäjiä, sillä jokaisen opiskelijan kohdalla tehtävät opintomerkinnät olisivat liian laaja työ keskitetysti tehtynä. Niinpä käyttöoikeudet on annettu yliopisto-opettajille, kuitenkin rajatusti. Erilaisia käyttöoikeustasoja palvelussa on rekisterin käyttäjille kaikkiaan 21. Käyttöoikeustasojen kanssa pystytään palvelussa rajaamaan hyvin tarkasti se, mihin tietoihin henkilöllä on pääsy, ja onko pääsy ainoastaan luku-tasoinen vai muokkaustasoinen. Oikeuksia rekisteröityjen poistamiseen ei palvelussa ole pääkäyttäjien lisäksi muilla käyttäjillä. Käyttöoikeuksia palveluun anotaan erillisellä lomakkeella. Oikeusanomukset käsitellään ja arvioidaan sekä oikeudet joko annetaan tai evätään palvelun pääkäyttäjien toimesta. Käyttöoikeudet palveluun annetaan oletusarvoisesti toistaiseksi voimassa olevina. Yllä kuvattu raportointiautomatiikka toimii nyt pääkäyttäjien työkaluna niissä tapauksissa, kun käyttöoikeuksia tulisi poistaa johtuen muutoksista työsuhteessa tai työnkuvassa. Varsinaista automatiikkaa tämä ei tunnusten käyttöoikeuksien hallinnointiin tuo, mutta tuo näkyväksi käyttöoikeuksia hallinnoivalle henkilölle muutokset, jotka voivat vaikuttaa käyttöoikeuksien tarpee-

seen.

Koska opiskelijarekisterin tapauksessa kyse on vanhasta, elinkaarensa päässä olevasta palvelusta, ei rekisteriin ole tehty varsinaista suoraa mahdollisuutta saada tuotettua rekisteröityä koskevia tietoja ulos palvelusta. Mikäli tietopyyntöjen määrä kuitenkin kasvaisi suureksi yliopistolla, olisi tällainen raportoinnin toiminnallisuus mahdollista luoda yksinkertaisella raportointi-toiminnallisuudella Turun yliopiston tietovaraston kautta. Tätä tutkimusta tehtäessä tietopyyntöjen määrä on kuitenkin ollut vielä niin vähäinen, ettei tällaista raportointityökalua ole vielä ollut tarvetta luoda, vaan tietojen manuaalinen hakeminen rekisteristä on ollut riittävä toistaiseksi. Myöskään varsinaista työkalua henkilötietojen sähköiseen toimittamiseen pyydettäessä toista rekisteriä varten ei ole palveluun kehitetty, mutta edelleä esitetty tietovarasto-yhteys mahdollistaisi myös tämän toteuttamisen.

Edellä mainittu opiskelijatietojen arkistointivelvoite rekisterissä on melko monimutkainen kokonaisuus palvelussa. Arkistointivelvoite perustuu arkistolakiin (831/94) 8 § [7], asetukseen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/99)[19] sekä niiden pohjalta laadittuun Turun yliopiston arkistonmuodostussuunnitelmaan, joka määrittää tarkemmin eri arkistoitavien asioiden ja asiakokonaisuuksien arkistointiajat ja -tavat. Arkistointitavalla tarkoitetaan tässä yhteydessä sitä, onko tiedon arkistointi mahdollista tehdä sähköisesti, vai edellytetäänkö arkistointia paperisena sähköisen arkistoinnin teknisten haasteiden vuoksi. Turun yliopistossa ollaan siirtymässä kohti sähköistä arkistointia enenevässä määrin, mutta hanke on tätä tutkielmaa kirjoitettaessa vielä vaiheessa, eikä sähköistä arkistointia voida näin vielä täysimitaisesti hyödyntää arkistointivelvoitetta täytettäessä.

Koska opiskelijarekisteri sijaitsee kokonaisuudessaan Turun yliopiston omassa hallinnassa ja palvelua ylläpidetään yliopiston oman henkilöstön toimesta, ei rekisterillä ole varsinaista henkilötietoja käsittelevää tahoa. Rekisteristä luovutetaan

tietoja rekisteröidyistä kansallista raportointia ja seurantaa varten käytössä olevaan Virta -palveluun ja Tilastokeskuksen käyttöön. Lisäksi Turun yliopiston ylioppilaskunta TYY ja Oy Frank Students AB vastaanottavat tietoja rekisteristä opiskelijakorttien myöntämisen perusteiden varmistamiseksi. Vastaavasti Ylioppilaiden terveydenhoitosäätiö opiskelijaterveydenhoidon oikeutuksen varmistamiseksi. Näiden lisäksi myös muut suomalaiset yliopistot ja Turun alueen ammattikorkeakoulut vastaanottavat tietoja rekisteröidyistä Joustavan opinto-oikeuden, eli JOO-opintojen suorittamisen mahdollistamiseksi.[9]

5.1.3 Opsu ja rekisteröidyn oikeudet

Vaikka opiskelijarekisteri onkin Turun yliopiston velvoitteiden täyttämisen kannalta välttämätön rekisteri ja yliopiston oikeutettu etu menee lain vaatimusten vuoksi rekisteröityjen oikeutetun edun edelle esimerkiksi juuri arkistointivelvoitteiden vuoksi, on rekisteröidyllä silti rekisteriin liittyen Tietosuoja-asetuksen edellyttämät oikeudet suurelta osin. Rekisteröidyllä henkilöllä on oikeus edellyttää virheellisten tietojen oikaisemista tai poistamista rekisteristä, mikäli hänen tietonsa rekisterissä ovat virheellisesti kirjattuja tai vääriä. Edellä kuvatusti rekisteröidyllä on mahdollisuus itsepalveluportaalin kautta tarkastella omia tietojaan rekisterissä, mutta Tietosuoja-asetuksen ja asetuksen viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/99) kautta rekisteröidyllä on oikeus saada tietoonsa myös ne tiedot itsestään, joita tuon palvelun kautta ei rekisteröidylle esitetä. Ja vaikka opiskelijarekisteriin ei olekaan toteutettu toiminnallisuutta, jolla rekisteröity saisi omat tietonsa siirrettyä sähköisesti toiseen rekisteriin niin halutessaan, on hänellä kuitenkin oikeus tällaista palvelus rekisterinpitäjältä vaatia.

Opiskelijarekisteristä on laadittu kattava tietosuojailmoitus, joka on saavutettavissa Turun yliopiston verkkosivujen kautta. Tietosuojailmoitus on rekisteröidyn saatavilla myös rekisteröidyn käyttöliittymän, Nettiopsun kautta.[9]

5.2 Henkilöstörekisteri

Turun yliopiston henkilöstörekisteri pitää sisällään kaikkien yliopiston henkilökuntaan kuuluvien henkilöiden perustiedot. Henkilörekisteri poikkeaa muista yliopiston ydinrekistereistä siinä mielessä, että se sijaitsee yliopiston oman palvelinympäristön ulkopuolella, palveluntarjoajan palvelimella. Koska rekisteri sisältää tiedot henkilöiden työsopimuksista, ei rekisteri sisällä varsinaisesti arkaluontoiseksi luokiteltavaa henkilötietoa, mutta rekisteröityjen kannalta hyvin suojattavaa tietoa kuitenkin, joten rekisterin suojauksen on hyvä olla taattu ja turvattu. Henkilöstörekisterin henkilötietojen käsittelyn oikeusperustana on katsottu olevan sopimus sekä lakisääteisen velvoitteen hoitaminen. Henkilöstörekisteri on olemassa, jotta yliopisto voisi täyttää tehokkaasti lakisääteiset velvoitteensa työntekijöiden työsopimusten, palkkatietojen, palkkioiden maksamisesta ja hallinnoimisesta.[10]

Henkilöstörekisterin osalta henkilötietojen käsittely on oikeastaan henkilötietojen säilyttämisen ohessa ainoa syy koko rekisterin olemassaololle. Tästä syystä henkilötietojen käsittelyyn tulee olla hyvin tarkat rajoitukset käyttöoikeuksien osalta. Henkilöstörekisteri on jaettu eri palveluihin käyttötarkoituksen mukaisesti. Personec F sisältää rekisteröityjen henkilötiedot sekä tiedot henkilöiden työsuhteesta, työstävapautukset, luottamustoimet, työuratiedot sekä muiden muassa rekisteröidyn pankki- ja verotustiedot. Rekisterin osana toimivat myös henkilöstön palvelussuhteen arviointidokumentit sisältävä Personec HR -palvelu sekä henkilöstön vuosilomien hallinnointiin takoitettu Personec ESS -palvelu. Rekisteröidyllä itsellään ei ole pääsyä varsinaiseen henkilörekisteriin, vaan rekisteröidyt pääsevät tarkastelemaan omia tietojaan tarvittavassa laajuudessa Personec HR ja ESS -palveluiden Internet-pohjaisten käyttöliittymien kautta. Esimiesasemassa toimivilla rekisteröidyillä on pääsy samojen käyttöliittymien kautta myös omien alaistensa henkilö- ja työsuhdetietoihin tarvittavassa laajuudessa.

Palveluun kirjauduttaessa käytetään yliopiston kertakirjautumispalvelua. Kir-

jautumista ei ole rajoitettu pelkästään yliopiston verkossa tapahtuvaksi, vaan palveluun kirjautuminen onnistuu miltä laitteelta tahansa ja mistä verkkoympäristöstä tahansa. Tietoliikenneyhteys palveluun muodostetaan SSL-sertifikaatilla suojattuna käyttäjän Internet-selaimelta.

Kuten yllä todettiin, käyttöoikeus koko henkilöstön henkilö- ja työsuhdetietoihin on hyvin rajatulla joukolla ihmisiä, jotka työskentelevät Turun yliopiston henkilöstöhallinnon työtehtävissä. Muiden käyttäjien osalta pääsy henkilötietoihin rajoittuu aina sen tiedekunnan, laitoksen tai yksikön mukaan, jossa henkilö työskentelee. Lähtökohtaisesti henkilöllä on pääsy vain omiin tietoihinsa palvelun käyttöliittymän kautta, mutta mikäli henkilöllä on määritettynä alaisia työsuhteessaan, pääsee hän kirjautuessaan näkemään myös alaistensa henkilötiedot. Lisäksi, mikäli henkilö toimii laitoksen tai tiedekunnan johtotehtävissä, on hänellä pääsy omien suorien alaistensa lisäksi myös näiden alaisuudessa mahdollisesti toimivien henkilöiden henkilötietoihin. Kuitenkin, esimerkiksi henkilöiden käymien arviointikeskusteluiden sisältöjä pääsee tarkastelemaan ainoastaan henkilön suora esimies.

5.2.1 Henkilöstörekisteri ja rekisterinpitäjän velvollisuudet

Rekisterin henkilötietojen käsittelyn oikeusperustaksi henkilöstörekisterissä on katsottu olevan sekä sopimus että toisaalta myös lakisääteisen velvoitteen hoitaminen. Rekisteriin kuuluvat ovat kaikki sopimussuhteessa tai entisessä sopimussuhteessa Turun yliopiston kanssa. Lakisääteisen velvoitteen hoitamisen alle katsotaan kuuluvan yliopiston työsopimussuhteisten henkilöiden henkilötietojen hallinnoinnin, sekä lain velvoittaman arkistointivelvoitteen täyttäminen.[10]

Rekisteröidystä palvelussa säilytettävien tietojen määrä on lähtökohtaisesti minimoitu vain työsuhteeseen liittyviin olennaisiin tietoihin palvelussa. Järjestelmätoimittaja edellyttää rekisterissään oleville tietokentille löytyväksi aina perustellun käyttötarkoituksen, jotta rekisteriin rakennettu tietojen käyttötarkoitusluokitusten

rakenne pystytään määrittämään. Luokituksiin on tosin jätetty olemaan luokitus myös asiakkaan vaatimusten mukaiselle luokitukselle, sillä järjestelmätoimittaja toimii kuitenkin vain rekisterin henkilötietojen käsittelijänä eikä niinkään varsinaisena rekisterinpitäjänä, jossa roolissa sen tehtävänä onkin mahdollistaa tietosuojan toteuttaminen rekisterissä ja auttaa tietosuoja-asetuksen edellyttämän tietosuojatason saavuttamisessa. Tietojen luokittelu palvelussa on tehty kahdessa tasossa. Toisaalta tietokentät luokitellaan tuotteen vaatimusten, lakisääteisyyden ja edellä mainitun asiakkaan vaatimusten mukaisesti. Tämän lisäksi tietokentät luokitellaan myös henkilötietojen arkaluontoisuuden mukaan asteikolla 0-3 tason 0 ollessa "ei henkilötietoa"ja toisen ääripään arvo 3 "arkaluontoista henkilötietoa". Tämä luokitus on tehty yhtälailla auttamaan rekisterinpitäjää Tietosuoja-asetuksen vaatimusten täyttämisessä.

Kuten yllä esitettiin, on pääsy henkilöstörekisteriin hyvin rajattu johtuen rekisterissä säilytettävistä tiedoista, kuten palkkatiedot. Varsinaiseen rekisterin ylläpitoosaan, Personec F:ään on pääsy rajattu mahdolliseksi vain yliopiston sisäverkosta. Yliopiston ulkopuolisesta verkosta pääsyyn on käytettävä VPN-yhteyttä tai yliopiston virtuaalityöpöytää. Järjestelmässä olevaan rekisteröidylle itselleen tarkoitettuun palveluun pääsy on huomattavasti vapaampaa, sillä pääsyä ei ole rajattu lainkaan erillisellä verkkokohtaisella estolla, vaan käyttäjälle riittää pääsy Internetiin. Palvelun kirjautuminen tapahtuu yliopiston kertakirjautumisjärjestelmän avulla, joten palvelun suojaustaso esimerkiksi salasanan osalta noudattaa yliopiston yleistä salasanapolitiikkaa.

Käyttöoikeudet rekisterin ylläpitoon on rajattu ainoastaan yliopiston Henkilöstöpalveluiden työntekijöille, joilla työnsä vuoksi on tarve tietoja päästä ylläpitämään. Palvelussa on henkilötietojen muokkaus rajattu jopa niin pitkälle, ettei rekisteröity pysty itse muokkaamaan henkilötietojaan edes hänelle suunnatun käyttöliittymän kautta. Rekisteröidyn on mahdollista päivittää henkilötietonsa, kuten puhelinnume-

ronsa ja nimi- tai osoitetietonsa muissa palveluissa, joista tiedot päivittyvät myös henkilöstörekisteriin.

Henkilötietojen käsittelystä syntyvä lokitus henkilöstörekisterissä ei aivan kaikilta osin vastaa tietosuoja-asetuksen vaatimuksia, sillä henkilötietojen käsittelyksi luokiteltavaa tietojen katselua ei palvelussa kerätä lokiin. Rekisterissä tehdyistä muutoksista sen sijaan lokidataa kerätään, samoin kuin järjestelmän sisään- ja uloskirjautumiset. Henkilötietojen katselun lokituksen puute on päädytty jättämään pois, sillä henkilötietojen ylläpitämisen mahdollisuus on palvelussa rajattu vain palvelun ylläpitäjille, joita katsotaan aina olevan hyvin rajallinen joukko. Lisäksi tietojen saanti on palvelussa rajattu käyttöoikeuksien avulla. Koska käyttöoikeuksien hallinnointi tapahtuu palvelussa manuaalisesti, eikä ole sidottu esimerkiksi automaattisesti identiteetinhallintajärjestelmän avulla työsopimukseen, katson tämän olevan riskialtis toteutus palvelussa.

5.2.2 Henkilöstörekisteri ja rekisteröidyn oikeudet

Tietosuoja-asetuksen myötä rekisteriin toteutettiin käyttäjille mahdollisuus päästä selailemaan ja tarvittaessa lataamaan omat rekisterissä olevat tietonsa. Varsinaisia tietopyyntöjä ei sen myötä palvelussa ole tarpeen tehdä niiden, joilla on olemassa aktiivinen työsopimus Turun yliopiston kanssa. Ne, joilta työsopimus on jo katkennut, mutta jotka yliopiston lakisääteisten velvoitteiden vuoksi ovat edelleen henkilöstörekisterissä, on mahdollista tehdä rekisteriin tietopyyntö yliopiston normaalin tietopyyntökäytännön mukaisesti. Rekisterissä olevien tietojen oikaiseminen tai poistaminen tapahtuu rekisterin ylläpitäjän toimesta ja rekisteröidyllä on oikeus tämän pyytämiseen. Kuitenkin yliopiston lakisääteiset velvoitteet asiakirjojen arkistoinnista rajoittavat tätä oikeutta.

Rekisteröidyn on mahdollista pyytää itseään unohdetuksi rekisteristä, mutta yliopiston lakisääteiset velvoitteet ajavat rekisteröidyn oikeuksien edelle, joten koko-

naan unohdetuksi henkilö ei rekisteristä voi tulla ennen kuin lakisääteisten tietojen säilytysaika määrää henkilötiedot poistamaan. Rekisteristä on mahdollista poistaa henkilötiedot poistamalla henkilö kokonaan tai palvelussuhdekohtaisesti. Oletusarvoisesti järjestelmä säilyttää henkilön palkkatiedot ja niiden myötä henkilön itsensä rekisterissä arkistonmuodostussuunnitelman mukaisen ajan, jonka jälkeen tiedot poistuvat automaattisesti.

Rekisteristä on laadittu asianmukainen tietosuojailmoitus, joka on saavutettavissa Turun yliopiston verkkosivujen kautta.[10]

5.3 Kontaktirekisteri

Turun yliopiston kokoisessa organisaatiossa on hyvin mittava määrä erilaisia kontaktirekistereitä, kun periaatteessa jopa kaikki työntekijöiden osoitekirjat voidaan mieltää sellaiseksi. Tässä tutkimuksessa keskityn kuitenkin kontaktirekisterin osalta yliopiston pääasialliseen, viralliseen kontaktirekisteriin, jossa sijaitsevat esimerkiksi yliopiston alumnit. Koska yliopiston erilaisten tapahtumien osallistujat, ja heistä syntyvät erilliset henkilörekisterit sijaitsevat kontaktien kanssa samassa palvelussa, käsittelen tutkimuksessani myös nämä rekisterit.

5.3.1 Palvelun tietoturvallisuus

Kuten luvussa kaksi 2 käytiin läpi, sijaitsevat yliopiston kontaktirekisteri ja tapahtumakohtaiset henkilörekisterit yliopiston käyttämässä Konsta –palvelussa. Konsta on avoimen lähdekoodin sisällönhallintajärjestelmän, DNN:n työkaluilla perustettu palvelu, joka käyttää tietokantanaan Microsoft:n SQL-tietokantaa. Palvelu sijaitsee Turun yliopiston omassa palvelinympäristössä, yliopiston virtuaalipalvelinalustalle sijoitetulla tietokantapalvelimella. Palvelusta on samalla virtuaalipalvelinalustalla myös testiympäristö, joka vastaa osittain tuotantoympäristössä sijaitsevaa

varsinaista palvelua, mutta on käyttöoikeusiltaan huomattavasti rajatumpi ja tietosisällöltään vanhentunut. Testiympäristöön päivitetään ajoittain tuotantoympäristön sisältö, kun esimerkiksi palveluun ollaan ottamassa käyttöön uutta toiminnallisuutta tai ominaisuutta, ja sen ilmenemistä ajantasaisella tietosisällöllä halutaan mallintaa. Tätä datapäivitystä ei kuitenkaan tehdä millään tavalla ajastetusti tai säännöllisesti. Kummankin palvelun tietoturva on toteutettu asianmukaisella, palvelinkäyttöön tarkoitetulla virustorjunta- ja palomuuriohjelmistolla. Itse tietokantapalvelimelle käyttöoikeuksia on vain ylläpitohenkilöstöllä. Palvelimelle voi kirjautua vain Turun yliopiston ylläpitoverkosta etätyöpöytäsovelluksella. Myös palvelun toimittajayrityksen nimetyillä työntekijöillä on pääsy palvelimille erikseen määritetystä IP-osoiteavaruudesta ja vain henkilökohtaisella tunnuksella, jolloin jokainen ylläpitotoimenpide palvelinympäristössä pystytään tarvittaessa todentamaan. Näiden myötä voidaan sanoa, että palvelun tietoturva on tekniseltä tasoltaan hyvällä tasolla ja toteutettu hallitusti. Myös tietosuoja-asetuksen palveluille asettamat vaatimukset on palvelussa lähtökohtaisen tietoturvan näkökulmasta huomioitu ja toteutettu vaatimukset täyttäen. Palvelua käytetään Internet-selaimella. Käyttäjät voivat kirjautua palveluun millä tahansa Internet-selaimella, palvelun käyttöä ei siis ole rajattu käytettäväksi vain tietyllä selaimella tai tietystä lokaatiosta tai verkkoympäristöstä käytettäväksi. Palvelinyhteys muodostetaan suojattuna.

Palveluun kirjaudutaan käyttäen Turun yliopiston kertakirjautumispalvelua, OpenAM:ia. Palvelu pohjautuu jo vuonna 2005 julkaistuun OpenSSO-pääsynhallinnan sovellukseen, joka myöhemmin eriytettiin kokonaan omaksi tuotteekseen. Näin palvelun pääsynhallinta on vahvasti eriytetty sisällönhallintajärjestelmän omasta tunnushallinnasta, mutta varsinaisesti palvelussa toimivat käyttäjät toimivat itse sisällönhallintajärjestelmän tunnuksilla, jotka päivitetään kertakirjautumisen yhteydessä OpenAM-pääsynhallintapalvelun antamien tietojen mukaisesti. Palvelussa hyödynnetään sisällönhallintajärjestelmän käyttöoikeusryhmiä, mutta ensisijaisesti käyttö-

oikeusryhmien jäsenyydet hallinnoidaan Turun yliopiston identiteetinhallintajärjestelmän tuottamien roolien kautta, josta tiedot käyttäjällä olevista rooleista päivitetään jokaisen käyttäjän tekemän kirjautumisen yhteydessä palveluun kertakirjautumistiedon mukana. Sisällönhallintajärjestelmän sisäisiä käyttäjäryhmiä on myös mahdollista käyttää palvelussa edellisten lisäksi, mutta tätä mahdollisuutta ei juuri ole palvelussa aktiivisesti käytetty. Identiteetinhallintajärjestelmä toimii täysin käyttäjätietojärjestelmien, eli henkilöstö- ja opiskelijatietojärjestelmien tuottamien tietojen varassa, jolloin niistä saadut tiedot esimerkiksi muutoksista käyttäjän rooleissa ja oikeuksissa kulkeutuvat ilman viivettä roolitietoja hyödyntävään palveluun, ja palvelun väärinkäytökset esimerkiksi palvelussuhteen muutoksen yhteydessä ovat käytännössä mahdottomia. Konsta-palveluun on toteutettu myös pelkästään sisällönhallintajärjestelmän käyttäjähallintaan toteutettuja käyttäjätunnuksia lähinnä ylläpidollisiin ja koulutustarkoituksiin. Näin on saatu varmistettua ylläpidon toimivuus myös siinä tapauksessa, että pääsynhallintapalvelussa on häiriö, joka estää normaalin ylläpitotyön toteuttamisen. Vastaavasti koulutustarkoituksessa sisällönhallintajärjestelmään paikallisesti tehdyt käyttäjätunnukset mahdollistavat erilaisiin rooleihin kohdistuvan kouluttamisen ilman, että koulutettaville pitää antaa etukäteen rooleja vastaavia käyttöoikeuksia ennen varsinaisen koulutuksen antamista. Ylläpito- ja koulutustunnuksia palveluun pystyvät luomaan vain palvelun ylläpitäjät, joita Turun yliopistossa on nykyisin kaksi – varsinainen pääkäyttäjä sekä hänen varahenkilönsä. Paikalliset koulutustunnukset on mahdollista poistaa välittömästi koulutuksen päätyttyä, tai koulutustunnusten salasanat voidaan nollata. Tunnusten lisäksi palveluun voidaan perustaa sisällönhallintajärjestelmään perustettuja käyttäjäryhmiä, joilla esimerkiksi tapahtumanhallinnan tapahtumien normaalia parempi suojaus on mahdollista toteuttaa. Lisäksi palvelun toimittajalla on palveluun vielä ylläpitäjää suuremmat käyttöoikeudet, jotta palvelun kehittäminen ja tietokantatason ongelmien ratkaiseminen olisi ylipäätään mahdollista.

5.3.2 Konsta ja rekisterinpitäjän velvollisuudet

Koska Konsta palveluna jakautuu moneen eri tyyppiseen henkilörekisteriin, on rekisteritietojen keräämisellekin ymmärrettävästi olemassa useampia syitä ja perusteita. Konstassa suurin henkilörekisterien massa kerääntyy tapahtumanhallinnan ympäristöön, jonne saattaa vuodessa kertyä yli 500 henkilörekisteriä (vuoden 2018 aikana 574 kappaletta tapahtumia, joissa yksi tai useampia osallistujia). Henkilörekisterillä tässä tarkoitetaan yliopiston järjestämää tapahtumaa, jonne ilmoittautuneelta osallistujalta on kerätty jonkinlaisia henkilötietoja, joiden avulla henkilö olisi tunnistettavissa. Palvelun omistajan, tekniset vastuuhenkilön sekä yliopiston tietosuojavastaavan näkemyksen mukaan tapahtumien henkilötietojen keräämisen oikeusperusteen katsottiin pohjautuvan sopimussuhteeseen, joka tapahtumaan ilmoittautuvan ja Turun yliopistolle syntyy tapahtumaan ilmoittautumisen myötä. Palvelun tietosuojailmoituksessa on määritetty lisäksi seuraamukset tämän sopimuksen täyttymisen edellytyksenä olevalle tietojen antamisesta kieltäytymiselle – yliopisto ei voi tällöin sitoutua tähän sopimussuhteeseen, eli käytännössä ottaa vastaan tapahtumaan ilmoittautumista.

Henkilökoulutukset yliopiston tapahtumanhallintapalvelussa ovat yhtäältä vastaavanlaisia tapahtumia ja muodostavat vastaavanlaisia henkilörekistereitä kuin tavalliset yliopiston tapahtumatkin. Henkilöstökoulutusten henkilötietojen käsittelyn ensisijaiseksi oikeusperusteeksi on kuitenkin katsottu työnantajan lakisääteisten velvollisuuksien täyttäminen. Työsopimuslain 2. luvun 1 §:n [20]yleisvelvoitteen mukaan työantajan on mahdollistettava työntekijän henkilökohtainen kehittyminen suoriutuakseen työssään ja annettava mahdollisuus kehittää itseään edetäkseen työurallaan. Toisaalta yliopisto saa koulutuskorvausta perustuen lakiin koulutuksen korvaamisesta (1140/2013). Tämän lain tarkoituksena on parantaa työnantajan mahdollisuuksia järjestää työntekijöilleen heidän ammatillista osaamistaan kehittävää koulutusta. Joihinkin henkilöstökoulutuksiin on mahdollista osallistua kuitenkin myös

yliopiston henkilökunnan ulkopuolisia henkilöitä, joiden osalta henkilötietojen käsittelyn oikeusperustaksi katsotaan yhtälailla sopimuksen syntyminen kuin yliopiston normaaleissakin tapahtumissa.

Kolmas Konsta-palvelun henkilörekisterikokonaisuus on kontaktirekisteri. Turun yliopistossa päädyttiin jakamaan kontaktirekisteri henkilötietojen käsittelyn oikeusperusteen suhteen osiin sen perusteella, mitä tietokokonaisuuksia henkilöstä on rekisteriin tallennettuna. Näitä niin kutsuttuja profiileita voi kontaktilla on yksi tai useampia, kuitenkin siis vähintään yksi. Mikäli tämän profiilin mukaisten henkilötietojen käsittelyn oikeusperusta on suostumus, kysytään rekisterissä olevalta kontaktilta suostumus henkilötietojen käsittelyyn. Toistaiseksi rekisterissä ei ole vielä yhtään tällaista tietokokonaisuuden mukaista profiilia, joten tarvetta suostumuksen kysymiselle ei vielä ole ilmennyt. Kontaktirekisteriin on perustettu tämän tutkielman kirjoittamiseen mennessä neljä erillistä profiilia – Turun yliopiston alumnit, mentorit, varainhankinnan lahjoittajat sekä yliopiston viestintäyksikön sidosryhmärekisteri. Näiden kaikkien rekisterien henkilötietojen käsittelyn oikeusperuste on katsottu olevan rekisterinpitäjän oikeutettu etu. Minkään näistä neljästä rekisteristä osalta ei voida katsoa rekisteröidyn etujen tai perusoikeuksien tai –vapauksien syrjäyttävän rekisterinpitäjän oikeutettua etua. Henkilötietojen säilyttämisen oikeusperusteet kaikkien yliopiston henkilörekisterien osalta on kuvattu tarkemmin alla olevassa taulukossa.

Taulukko 5.1: Konstan sisältämien henkilörekisterien oikeusperusteet

Rekisteri / Käyttöoikeusperuste	Suostumus	Sopimus	Lakisääteiset velvoitteet	Yleinen etu	Oikeutettu etu
Alumnirekisteri					x
FTPF sidosryhmärekisteri					x
Henkilöstökoulutukset		x	x		
INVEST sidosryhmärekisteri					x
Lahjoittajarekisteri			x		x
Mentorirekisteri					x
Oik.tdk. sidosryhmärekisteri	x				x
Rekryn sidosryhmärekisteri					x
Tapahtumanhallinta		x			
Viestinnän sidosryhmärekisteri					x

Oikeutetun edun peruste rekistereissä, joissa henkilötietojen säilytysperusteeksi on määritetty oikeutettu etu ovat:

- Alumnirekisteri - Rekisterinpitäjän oikeutettu etu perustuu yliopiston työntekijöiden mahdollisuuteen toteuttaa yhteiskunnallista vuorovaikutusta ja ylläpitää käsittelyn tarkoituksessa kuvattua yhteyttä entisiin opiskelijoihin ja työntekijöihin.

- Mentorirekisteri - Turun yliopistolla ja rekisteröidyillä on merkityksellinen suhde, joka perustuu rekisteröidyn vapaaehtoiseen osallistumiseen yliopiston mentorointiohjelmaan tai vaihtoehtoisesti rekisteröidyn ilmoittamaan kiinnostukseen toimia mentorina.

- Varainhankinnan lahjoittajat - Turun yliopistolla ja rekisteröidyllä on merkityksellinen suhde, joka perustuu rekisteröidyn Turun yliopistolle tekemään lahjoitukseen.

- Turun yliopiston viestinnän sidosryhmärekisteri - Yliopistolla ja rekisterissä olevalla henkilöllä on merkityksellinen suhde. Rekisteriin merkityt ovat yliopis-

ton näkökulmasta asiakkaan tai alaisen asemassa liittyen yliopiston kolmanteen tehtävän eli yhteiskunnallisen vuorovaikutuksen toteuttamiseen. Henkilö on otettu mukaan rekisteriin asemansa, työtehtävänsä tai yliopiston kannalta merkittävän sidosryhmäyhteyden vuoksi.

- Hanke-luontoisilla rekistereillä, kuten Food Tech Platform Finland sekä INVEST-sidosryhmärekisteri sekä tiedekuntien sidosryhmärekistereillä on katsottu oikeusperustan olevan oikeutettu etu yhtälailla merkityksellisen suhteen ja yhteiskunnallisen vuorovaikutuksen myötä muodostuneen sidosryhmäyhteyden kautta.[13]

Jotta tietosuoja-asetuksen ehdot rekisterissä täyttyvät, on rekisterinpitäjä velvollinen huolehtimaan joistain vaatimuksista. Henkilötietojen käsittely on rekisterissä oltava mahdollisimman vähäistä ja tämä vaade koostuu kahdesta eri osatekijästä. Osittain on huolehdittava henkilötietojen pääsy vain niille käsittelijöille, joilla on tarve henkilötietoja käsitellä, ja toisaalta heidänkin tulisi käsitellä henkilötietoja vain todellisessa tarpeessa. Kontaktirekisterin rakenne koostuu kaikille profiileille yhteisistä kontaktin yhteystiedoista, sekä kunkin profiilin alle kootuista profiilikohtaisista erityistiedoista. Henkilötietojen käsittelyn laajuutta on rajoitettu vastaavasti yleisiin yhteystietoihin ja profiilikohtaisiin erillisillä käyttöoikeusrooleilla niin, että kontaktinhallintaan kirjautuva käyttäjä näkee vain ne henkilöön liittyvät tiedot rekisteröidyistä, jotka hänen kuuluukin nähdä. Ja ne profiilit ja niiden sisältämät henkilötiedot, joihin käyttäjällä ei ole käyttöoikeutta, ovat vastaavasti käyttäjältä piilotettuina. Myös itse kontaktinhallinta on siis piilotettu valtaosalta käyttäjiä ja käyttöoikeudet myönnetään erillisellä käyttöoikeusroolilla.

Tapahtumien osalta käyttöoikeudet muodostetaan aina tapahtuman perustajan toimesta. Kaikki yliopiston tapahtumanhallintaan tehdyt tapahtumat ovat kaikille henkilökuntan kuuluville avoimia ja muokattavissa, kunnes tapahtumaan tulee ensimmäinen osallistuja. Siinä vaiheessa tapahtumasta katsotaan muodostuvan hen-

kilörekisteri, ja tapahtuman käyttöoikeudet rajoittuvat automaattisesti vain tapahtuman perustajaan, eli omistajaan. Tapahtuman muodostamaan henkilörekisteriin voi kuitenkin olla tarve päästä muidenkin henkilöiden kuin rekisterinpitäjän, jolloin hänelle voidaan antaa erilliset oikeudet lisäämällä hänet tapahtuman resurssiksi. Mikäli henkilön tarve päästä henkilörekisteriin päättyy, jää vastuu käyttöoikeuksien poistamisesta tapahtuman perustajalle, joka toimii rekisterinpitäjän edustajana tässä henkilörekisterissä. Mikäli henkilön käyttöoikeus yliopiston käyttäjätunnukseen päättyy, estyy häneltä myös pääsy ko. tapahtumaan ja sen sisältämään henkilörekisteriin. Muutokset työsopimuksessa eivät sen sijaan katkaise pääsyä tapahtumaan. Henkilöstökoulutukset noudattavat muutoin samaa menettelyä, mutta toisin kuin tavallisen tapahtumanhallinnan kanssa, muutokset työsopimuksessa katkaisevat oikeuden henkilöstökoulutusten tapahtumanhallintaan, ja käyttöoikeus on lisättävä henkilölle erikseen uudelleen.

Kontaktirekisteristä kontaktit löytyvät henkilöhaun avulla. Hakutulokset tuodaan käyttäjälle listana, jossa on henkilön nimi, mahdollinen sähköpostiosoite sekä mahdollinen puhelinnumero. Mikäli hakutulosten määrä on runsas, palautetaan käyttäjälle vain kappalemäärätieto saaduista hakutuloksista varsinaisten henkilötietojen sijaan. Jotta varmistuttaisiin käytön rajoittuvan vain välttämättömään käyttöön, muodostuu jokaisesta palvelussa suoritetusta hausta merkintä palvelun käyttölokiin. Merkintään tallennetaan hakuehto, jolla kyseinen lista kontakteja on haettu. Erillisestä kontaktikortin käsittelystä ei sen sijaan lokimerkintää tule. Hakutulosten lokimerkinnästä on kuitenkin mahdollista palauttaa tieto henkilöistä, joiden henkilötietoja kyseinen käyttäjä on käsitellyt. Tapahtumanhallinnasta ei kerätä vastaavaa lokitietoa henkilötietojen käsittelystä. Tämä johtuu siitä, että tapahtuman alle sijoitettu henkilörekisteri on huomattavasti lyhytikäisempi kuin varsinaisen kontaktinhallinnan henkilörekisteri ja lisäksi pääsy henkilötietoihin on valmiiksi paljon rajatummalla käyttäjäjoukolla. Henkilötietoihin tehdyt muutokset sen sijaan loki-

tetaan kaikki. Henkilöstökoulutukset eivät tässä suhteessa poikkea mitenkään muista yliopiston tapahtumista. Ainoastaan pääsy tapahtumiin on vielä rajatumpi kuin muissa tapahtumissa, mutta henkilötietoja sisältäviin tapahtumiin pitää myös henkilöstökoulutuksissa määrittää rekisterin käyttäjät erikseen.

Rekisteröidystä tulisi tietosuoja-asetuksen mukaan olla henkilörekisteriin tallennettuna vain oleellinen tieto. Perus yhteystietojen lisäksi ei rekisteröidystä kontaktirekisterissä tallenneta kuin syntymäaika ja sukupuoli, mitkä nekään eivät ole pakollisia täytettäviä tietoja. Kunkin profiilin osalta kerättävät tiedot määritellään erikseen kuitenkin niin, että profiilin alle kerätään vain kuhunkin tarkoitukseen oleellinen tieto. Tapahtumien osalta rajausta kerättävistä henkilötiedoista ei henkilörekisteriin edes voi tehdä rekisterin luonteen vuoksi. Tapahtumien sisältämät henkilötiedot kuitenkin kerätään aina henkilöltä itseltään, joten rekisteröidyn tietämättä ei henkilörekisteriin ole edes mahdollista kirjata tietoja. Paitsi jos tapahtuman omistaja täyttää henkilön rekisteröinnin tapahtumaan itse rekisteröidyn puolesta. Henkilötiedot, jotka rekisteröidystä tapahtumaan ilmoittautumisen yhteydessä kerätään, pohjautuvat samoihin yhteistietoihin, joista kontaktirekisterin puolella muodostuu henkilöstä kerättävät, kaikille yhteiset henkilötiedot. Näiden lisäksi kuhunkin tapahtumaan on kuitenkin erikseen mahdollista määrittää lisäkysymyksiä, joissa tapahtuman omistaja tai hänen nimeämänsä resurssi voivat kysyä rekisteröidyltä käytännössä mitä tahansa. Näiden tietojen keräämistä on käytännössä mahdotonta itse palvelussa teknisesti rajata niin, ettei itse palvelun käyttö sen varsinaiseen käyttötarkoitukseen häiriintyisi tai estyisi. Jokaisen tapahtuman omistaja on kuitenkin Turun yliopiston, eli rekisterinpitäjän edustajana tässä rekisterissä ja sen myötä varsinaisessa vastuussa kerättävistä henkilötiedoista ja niiden olennaisuuden varmistamisesta rekisterinpitäjän lukuun. Toki lopullinen vastuu on varsinaisella rekisterinpitäjällä, eli yliopistolla. Henkilöstökoulutukset eivät muodosta tässä suhteessa poikkeusta muihin tapahtumiin, vaan kerättävät henkilötiedot noudattavat samaa

mallia myös henkilöstökoulutuksissa.

Rekisterissä säilytettävien henkilötietojen on oltava ajantasaisia ja täsmällisiä. Kontaktirekisterin henkilötietojen ylläpitämiseen on yhtäläiset oikeudet kaikilla rekisterin käyttäjillä, jolloin yhden tekemät muutokset ja päivitykset henkilötietoihin pitävät ne ajan tasalla muidenkin osalta. Yksinkertaisimmillaan yhteystietojen päivityspyyntö tapahtuu henkilötietojen käsittelijän lähettämän lomakkeen kautta, josta rekisteröity pääsee itse muuttamaan mahdolliset päivittyneet tietonsa ja poistamaan vanhentuneet tiedot. Kontaktinhallinnan palvelussa on lisäksi olemassa oma käyttöliittymä rekisteröidylle, jonka kautta yhteystietoja on myös mahdollista päivittää. Tähän kontaktiportaali –palveluun voi rekisteröity itse tilata itselleen kirjautumislinkin antamalla palveluun sähköpostiosoitteensa, joka hänestä on rekisteriin tallennettu. Palvelu lähettää kirjautumislinkin ja salasanan annettuun sähköpostiosoitteeseen. Salasana kullekin rekisteröidylle on satunnaisesti arvottu merkkisarja kirjaimia ja numeroita. Pituudeltaan salasana on neljätoista merkkiä pitkä, minkä mitan on katsottu olevan jo kyllin tietoturvallinen. Itse kontaktiportaalin kirjautumissivulla on fail2ban –tyyppinen automatiikka vahtimassa, jos kirjautumisyrityksiä tulee tietystä IP-osoitteesta liikaa. Tällöin kirjautuminen estetään määräajaksi. Näin on estetty niin sanottujen sanakirjahyökkäysten käyttäminen kirjautumisessa. Palveluun liittyviä palvelupyyntöjä, kuten juuri henkilötietojen muuttamisen tai poistamisen pyyntöjä varten myös rekisteröidyillä on käytössään palvelupyyntölomake, jonka kautta tukipyyntöjä rekisterinpitäjän tukipalveluun voi luoda. Kontaktiportaalin kautta rekisteröidyn on mahdollista pyytää myös rekisteriin tallennettuja henkilötietojaan itselleen tai pyytää unohdetuksi tulemista rekisteristä. Henkilötietojen keräämistä varten luovutettavaksi on palveluun tehty automatiikka, joka kerää kaikki kyseistä rekisteröityä henkilöä koskevat tiedot koko rekisteristä. Tämä koskee myös henkilön tekemiä tapahtumailmoittautumisia, mikäli kontaktihenkilö on ilmoittautunut yliopiston tapahtumaan niin sanottuna kohdistettuna henkilönä, eli

ilmoittautuminen voidaan kohdistaa nimenomaan henkilön kontaktikorttiin. Mikäli sama henkilö on rekisterissä useampaan kuin yhteen kertaan, eli henkilöstä on enemmän kuin yksi kontaktikortti palvelussa, ei palvelu osaa koota näitä henkilötietoja samaan raporttiin. Tällöin eri kontaktikorttia koskevat henkilötiedot on raportoitava rekisteröidylle erikseen, tai mikäli useammalle kontaktikortille palvelussa ei ole loogista perustetta, poistettava duplikaattina muodostuneet kontaktikortit. Mikäli henkilö on ilmoittautunut Turun yliopiston tapahtumanhallintajärjestelmän kautta tapahtumaan niin sanotun avoimen lomakkeen kautta, eli tunnistamattomana, ei henkilön ilmoittautumista tällöin voida yhdistää henkilötietoja kokoavaan raporttiin. Tämä on täysin mahdollista, sillä ilmoittautumislomakkeet ovat pääsääntöisesti avoimia lomakkeita, jonne voi ilmoittautua samoilla tiedoilla, kuin mitä kontaktikortille henkilöstä on ilmoitettu, mutta palvelussa ei ole olemassa automatiikkaa, joka yhdistäisi nämä kaksi erillistä identiteetti-ilmentymää. Tästä syystä myös tapahtumiin osallistumiset ja niissä säilytettävät mahdolliset henkilötiedot on raportoitava henkilölle erikseen. Tähänkin on palvelun osana olemassa oma erillinen raportointityökalu. Tapahtumanhallinnassa henkilötietojen ajantasaisuutta ei varsinaisesti tehdä, sillä henkilötietojen säilyttäminen rekisterissä on lopulta verrattain lyhytaikaista. Tavallisesti henkilörekisterin henkilötietoja ei tapahtuman päättymisen jälkeen käytetä mihinkään, vaan ne poistetaan tapahtumasta säilytysajan umpeuduttua. Mikäli henkilön tiedot siirretään tai kopioidaan tapahtumasta toiseen tapahtumaan ilmoittautumisen pohjatiedoiksi, saa rekisteröity kuitenkin tiedot päivitettäväkseen ilmoittautumisen yhteydessä. Henkilöstökoulutuksissa rekisteröidyn henkilötiedot pohjautuvat henkilön kirjautumisen yhteydessä antamiin tietoihin, eli osallistuminen kohdistetaan aina joko ilmoittautumisen yhteydessä tai jälkikäteen koulutustapahtuman omistajan tai resurssin toimesta henkilöstöstä palvelussa ylläpidettävään kontaktirekisterin osaan. Kontaktirekisteri taas päivitetään joka kerta henkilön kirjautuessa Konsta –palveluun sisään, jolloin sen ajantasaisuus varmiste-

taan.

Henkilötietoja saa henkilörekisterissä säilyttää ainoastaan sen aikaa, kun rekisteröityä on tarvetta säilyttää rekisterissä. Tarpeen päättyessä tulisi rekisteröidyn tiedot poistaa rekisteristä. Konsta-palvelun kontaktirekisterissä tämä tarve määräytyy kontaktikorttiin liitettyjen profiilien perusteella. Jos profiilin tarve poistuu kontaktilta, poistetaan koko kyseinen profiili myös. Jos kontaktille ei jää jäljelle tämän jälkeen enää yhtään profiilia, poistetaan koko kontaktikortti. Kontaktin profiileista alumneille säilytysajaksi on määritetty niin kauan kuin kontaktihenkilö haluaa jatkaa jäsenyyttään alumniverkostossa. Alumnius ei ole henkilölle välttämätöntä eikä tietojen säilyttämiselle on yliopistolla varsinaista pakkoa tai vaatimusta, joten kuuluminen alumnirekisteriin on täysin rekisteröidyn itsensä päätettävissä. Lahjoittajatiedon osalta henkilötietojen säilytysajaksi on määritetty 10 vuotta viimeisimmästä lahjoitustapahtumasta. Tämän ajan kuluttua henkilöstä poistetaan muut henkilötiedot rekisteristä, mutta rekisteröidyn nimi ja ilmoitettu paikkakunta ovat pysyvästi säilytettäväksi määritettyjä henkilötietoja. Mentorien profiilissa henkilötietoja on määritetty säilytettäväksi seitsemän vuotta sen kalenterivuoden lopusta, jolloin henkilö on toiminut mentorina tai ilmoittanut halukkuudestaan toimia mentorina. Turun yliopiston viestinnän sidosryhmä –profiilissa henkilötietojen säilytystarpeen on määritetty päättyvän, kun sidosryhmäyhteistyö henkilön kanssa päättyy, tai henkilö itse haluaa henkilötietonsa rekisteristä poistettavan. Henkilötietojen säilytysaika rekisterissä ei siis ole yksiselitteisesti määritettävissä, vaan riippuu aina rekisterin luonteesta ja käyttötarkoituksesta. Tapahtumanhallinnan osalta tietosuojaselosteessa on määritetty tapahtumien säilytysaika. Säilytysaika voi vaihdella tapahtuman luonteen mukaan. Pääsääntöisesti tapahtumien henkilörekistereitä säilytetään yhden vuoden ajan tapahtuman päättymisestä, jonka jälkeen tapahtuman osallistujat anonymisoidaan. Tapahtuman säilytysaika voi poiketa kuitenkin tästä, mikäli lainsäädännölliset velvoitteet edellyttävät tapahtuman osallistujatietojen säilyttämistä

pidempään. Esimerkiksi Turun yliopiston järjestämä täydennyskoulutus on tällainen poikkeus. Tapahtuman henkilörekisterin säilytysaika määritetään tapahtuman perustiedoissa tehtävän luokituksen avulla. Tapahtuman osallistujien anonymisointi tapahtuu automaattisesti suoraan tietokantaan tehtävällä poistoajolla. Henkilöstökoulutukset poikkeavat henkilötietojen säilytysajan suhteen merkittävästi yliopiston muista tapahtumista, sillä Turun yliopiston arkistonmuodostussuunnitelmassa on määritetty henkilöstökoulutusten osallistujalistojen säilytysajaksi 15 vuotta. Tämän säilytysajan täytyttyä henkilöstökoulutusten henkilörekistereille tehdään vastaava anonymisointi suoraan tietokantaan kuin muillekin yliopiston tapahtumille.

Kuten edellä esitettiin, on Konstan eri henkilörekisterien käyttöoikeudet määritetty erikseen käyttäjällä olevaan sopimukseen liitettynä ja käyttäjällä on pääsy vain niihin henkilötietoihin, mihin hänellä on määritetty olevan tarvetta. Koska jokaisella käyttäjällä on oikeus muokata rekisteröidyn henkilötietoja, on hänellä myös oikeus ja mahdollisuus poistaa henkilö tai osa hänen tiedoistaan rekisteristä. Jokaisesta rekisteriin tehdystä muokkauksesta syntyy kuitenkin lokimerkintä palveluun, ja mahdollisen väärinkäytöksen tai vahingon myötä tapahtuneen tietojen tuhoamisen merkitys on sen myötä vähäinen, koska tarvittaessa tällainen tieto saadaan palautettua ennalleen.

Tapahtumaan rekisteröityjen henkilöiden henkilötietoja palvelussa pääsee muokkaamaan, jos käyttäjällä on käyttöoikeudet myös yliopiston kontaktirekisteriin. Mikäli käyttöoikeuksia ei ole, pääsee käyttäjä muokkaamaan kuitenkin henkilön tekemää ilmoittautumista, ja korjaamaan siinä yhteydessä mahdolliset virheelliset tiedot käyttäjästä. Rekisterinpitäjällä tai hänen nimeämällään rekisterin käyttäjällä on mahdollista poistaa rekisteröity henkilö tapahtumasta, mutta poistamisesta, sekä poistetuista henkilötiedoista jää kuitenkin lokimerkintä palveluun, jonka pohjalta rekisteröity olisi mahdollista palauttaa takaisin tapahtumaan mahdollisen väärinkäytöksen tapauksessa. Henkilön poistaminen tapahtumasta on tehty monivaiheiseksi –

ensin henkilö siirretään tilaan Poistettu, sen jälkeen poistettaessa hänet siirretään tilaan Alustava. Vasta tämän jälkeen tehty poistaminen poistaa henkilön rekisteröinnin lopullisesti. Näin palvelussa on pyritty minimoimaan vahingossa tapahtuva henkilön poistaminen rekisteristä.

Palvelussa on erikseen määritetty henkilön merkitseminen kuolleeksi sekä henkilön poistaminen. Näin estetään kuolleen henkilön perustaminen vahingossa uudelleen rekisteriin rekisterin käyttäjän toimesta. Palvelu antaa erillisen ilmoituksen, jos rekisterissä kuolleeksi merkittyä henkilöä yritetään perustaa uudelleen. Rekisteröidyn poistaminen rekisteristä siirtää henkilön vasta palvelussa olevaan Roskakoriin, jonne tavallisilla käyttäjillä ei ole pääsyä. Tämän myötä myös vahingossa tai tahallisesti väärinkäyttötarkoituksessa tehty rekisteröidyn poistaminen on mahdollista kumota järjestelmän ylläpitäjän toimesta. Tämä koskee tietysti vain tavallisten käyttäjien tekemiä poistamisia – tietosuoja-asetuksen määrittämä henkilön unohtaminen rekisteristä ei jätä häntä tietokantaan lainkaan, vaan hänet poistetaan lopullisesti. Poistettu –tilassa olevia käyttäjiä voidaan myös poistaa pysyvästi henkilörekisteristä ja tietokannasta, mutta tähän ei palvelussa ole rakennettu varsinaista automaatiota. Tähän poistamiseen olisi palvelussa varsin helppo tehdä myös automaatio, jonka katson olevan selkeä kehitysehdotus tietosuoja-asetuksen kokonaisvaltaisen täyttämisen saavuttamiseksi. Samoin rekisterinpitäjän tulisi määrittää aika, joka kuolleeksi merkittyjä henkilöitä palvelussa säilytetään ja rekisteriä kuolleista henkilöistä tulisi yhtä lailla siivota määritetyn säilytysajan mukaisesti. Näiden lokimerkintöjen ja poistamisen oikeuksien rajoittamisen lisäksi palvelun käyttämästä tietokannasta otetaan säännöllisesti varmuuskopio. Tämä varmuuskopiointi tehdään joka yö virtuaalisoidun palvelimen tilannekuvana, eli ”snapshot” –kuvana, josta palvelimen sen hetkinen tilanne on mahdollista palauttaa siihen hetkeen, kun tilannekuva palvelimesta on otettu. Mikäli rekisteristä on poistettu tahallisesti tai vahingossa jotakin, mikä ehdottomasti halutaan palauttaa, on palauttaminen mahdollista tehdä palaut-

tamalla tuo tilannekuva palvelusta. Lokimerkinnät palvelussa toimivat siis myös tietosuoja-asetuksen vaatimusten täyttämisen osoitusvelvollisuuden täyttämisessä, joka rekisterinpitäjän myös on kyettävä täyttämään.

Koska Konsta-palvelun toimittajalla on pääsy palveluun ja sen sisältämiin eri henkilörekistereihin, on toimittajan kanssa tehty sopimus henkilötietojen käsittelystä palvelussa. Itse sopimuksen lisäksi toimittaja on velvoitettu ylläpitotyössään käyttämään Turun yliopiston käyttäjähallintaan tehtyjä käyttäjätunnuksia, jotka sellaisenaan noudattavat samaa yliopiston käyttösääntö- ja tietoturvapolitiikkaa kuin muutkin yliopiston käyttäjätunnukset. Kullakin toimittajan ylläpitäjällä on oma henkilökohtainen tunnus, jonka salasanan hän saa vaihdettua omilla verkkopankkitunnuksillaan, tai muulla Turun yliopiston identiteetinhallintajärjestelmän tarjoamalla vahvan tunnistautumisen menetelmällä. Näin menetellen rekisterinpitäjän ominaisuudessa Turun yliopiston edustajalla on aina mahdollista osoittaa, kuka henkilö milloinkin on palvelussa henkilötietoja käsitellyt. Myös tunnusten ja käyttöoikeusien katkaiseminen esimerkiksi mahdollisessa väärinkäytöstapauksessa on helpompaa, kuin käytettäessä yhteiskäyttötunnuksia usean henkilön toimesta. Henkilötietojen käsittelijän ja rekisterinpitäjän välillä tulee olla sopimus henkilötietojen käsittelyn ehdoista. Sopimuksessa tulee määritellä, miten ja millä ehdoilla käsittelijä saa henkilötietoja käsitellä ja mitä ehtoja ja edellytyksiä käsittelijältä edellytetään. Turun yliopiston on solminut palvelun toimittajan, eTaika Oy:n kanssa sopimuksen toukokuussa 2018. Sopimuksessa määrätään, että sekä henkilörekisterin pitäjä, että osaltaan käsittelijä sitoutuvat noudattamaan lainsäädäntöä sekä Euroopan yleistä tietosuoja-asetusta ja niiden määrittämiä velvoitteita.

5.3.3 Konsta ja rekisteröidyn oikeudet

Tietosuoja-asetus toi näkyvämmin esille rekisteröidyn oikeuksia henkilötietoja sisältävään rekisteriin liittyen. Osa rekisteröidyn oikeuksista kerrotaan hänelle tieto-

suojailmoituksessa, osa taas ilmenee yksinkertaisesti rekisteröidyn oikeutena saada tietoja tarvittaessa tietosuojailmoituksessa ilmoitetuilta rekisterin yhdyshenkilöiltä. Konsta –palvelussa tietosuojailmoitus löytyy palvelun jokaisella sivulla sivun alalaidasta löytyvän linkin kautta, joten rekisteröitävä henkilö saa tarvittaessa kootusti tiedot rekisteripitäjästä, henkilötietojen keräämisen periaatteista ja muusta tietojen keräämiseen liittyvästä, kuten käyttötarkoituksesta. Varsinaiset tietosuojailmoitukset Turun yliopistossa on koottu yhden sivustokokonaisuuden alle julkisilla verkkosivuilla. Sivuille on siis esteetön pääsy miltä tahansa laitteelta selainriippumattomasti.

Kuten yllä kuvattiin, rakentuu Konsta-palvelun tietosuojailmoitus yhdestä pääasiallisesta tietosuojailmoituksesta, jossa kootaan palvelussa olevien erillisten rekisterien yhteiset asiat yhden ilmoituksen alle. Koska eri henkilörekisterit palvelussa poikkeavat toisistaan niin merkittävästi rekisteröinnin tarpeen, käsittelyn perustan sekä henkilöstä rekisteriin mahdollisesti kirjattavien henkilötietojen osalta, muodostetaan jokaiselle eri tyyppiselle henkilörekisterille oma tietosuojailmoituksensa varsinaisen tietosuojailmoituksen alle. Tällä menettelyllä on mahdollistettu myös rekisterikokonaisuuden jatkokehittäminen niin, ettei palvelun pääasialliseen tietosuojailmoitukseen tarvitse tehdä toistuvasti muutoksia, joista tulisi myös informoida rekisteröityjä henkilöitä. Pidän tätä toteutustapaa hyvänä ratkaisuna palvelulle, sillä se ei nimenomaan sido rekisterinpitäjää liikaa ja palvelun läpinäkyvyyttä voidaan kohdistaa ja esittää henkilölle juuri sen mukaisesti kuin juuri hänen osaltaan on tarpeen. Tämä tekee tietosuojaselosteesta myös hyvin kevyen ja selkeän nimenomaan rekisteröidyn kannalta.

Pääasiallisesti Turun yliopiston kontaktirekisterin tiedot on saatu rekisteröidyiltä itseltään. Suurimmaksi osaksi rekisteri koostuu toistaiseksi Turun yliopiston alumneista, jotka ovat valmistuessaan tutkintoon hyväksyneet tietojensa liittämisen tällaiseen kontaktirekisteriin. Mikäli valmistuva opiskelija ei tätä hyväksymistä anna,

ei hänen tietojaan myöskään rekisteriin siirretä. Siirto rekisteriin on syyskuusta 2015 lähtien tapahtunut automaattisesti opiskelijatietojärjestelmä Opsussa opiskelijasta olevilla tiedoilla. Tätä ennen alumniksi on voinut rekisteröityä Internet-lomakkeella, jollainen edelleen myös nykyisessä palvelussa on käytössä niitä henkilöitä varten, jotka eivät ole valmistuneet nykyisen suorasiirto –toiminnallisuuden aikaan. Koska henkilöt ovat ennen tämän siirron suorittamista antaneet hyväksyntänsä rekisteriin liittymiselle, voidaan myös olettaa henkilöiden tietävät kuuluvansa tähän rekisteriin. Tässä tapauksessa ei ole kuitenkaan katsottu rekisteriin kuulumisen olevan suostumukseen perustuva hyväksyntä rekisteröidyltä, vaan alumniuden on katsottu olevan yliopiston oikeutettu etu. Näin ollen myöskään näitä henkilöiltä saatuja suostumuksia ei olisi välttämätöntä säilyttää, sillä todistusvelvollisuutta suostumuksesta ei tarvita. Rekisteröidyllä on koska tahansa oikeus ja mahdollisuus vaatia tietojensa poistamista rekisteristä, koska yliopiston kontaktirekisterin alaisuudessa ei toimi yhtään sellaista rekisteriä, johon voitaisiin katsoa olevan esimerkiksi lakiin perustuva säilytysvelvollisuus. Poikkeuksen tähän muodostavat palvelun kautta tapahtuvat yliopiston varainhankinnan lahjoitukset, henkilöstön kehittämisen suorittamat koulutukset ja niiden osallistujalistat sekä palvelun tapahtumanhallinnan kautta tehtävät täydennyskoulutuksen ilmoittautumiset.

Palveluun rekisteröidyllä henkilöllä on tietosuoja-asetukseen pohjautuen oikeus päästä tarkastelemaan itsestään rekisteriin tallennettuja tietojaan ja niiden ollessa väärät tai vanhentuneet, oikeus pyytää niiden oikaisemista. Rekisteriin tallennetut tiedot ovat kuitenkin lähes poikkeuksetta henkilön itsensä antamia ja näin mahdollinen virhe henkilön tiedoissa on lähtöisin rekisteröidyltä itseltään, tai aiheutunut henkilön tiedoissa tapahtuneista muutoksista. Varsinaisen kontaktinhallinnan osalta rekisterissä on olemassa myös itsepalveluportaali, jota kautta rekisteröidyn olisi mahdollista koska tahansa tarkistaa tietonsa rekisterissä niiltä osin kuin tiedot on määritetty rekisteröidylle julkaistavaksi. Palveluun liittyvää kirjautumiskäytäntöä

ja sen tietoturvallisuutta on käsitelty tässä tutkielmassa aiemmin. Palvelussa olevista eri henkilörekistereistä ainoastaan viestinnän sidosryhmärekisterin sisältämiä tietoja ei ole asetettu rekisteröidylle itselleen julkaistavaksi, sillä niiden sisältö liittyy lähinnä henkilöiden käsittelyyn yliopiston sisäisesti, kuten kuuluminen yliopistoon liittyvien virallisten juhlatilaisuuksien kutsulistoihin tai vastaaviin, joka tieto rekisteröidylle itselleen ei ole merkityksellistä.

Pyydettäessä rekisteröidyn henkilötietoja, on hänet helppo löytää palvelusta sen hakutoimintojen avulla. Henkilöstä ei palveluun kerätä henkilötunnusta kuin varainhankinnan lahjoitusten yhteydessä, joten henkilön tekemän tietopyynnön yhteydessä on henkilöltä itseltään satava joitain tunnistetietoja, joilla hänet on mahdollista rekisteristä löytää. Rekisteröidyn tiedot saadaan palvelusta toimitettua suoraan XML-muotoisena tiedostona, jonka avulla tiedot saadaan pyydettäessä siirrettyä toiseen sähköiseen rekisteriin ja toisaalta tällä tiedostolla rekisteröidyn tiedot on mahdollista toimittaa rekisteröidylle sähköistä kanavaa pitkin niin pyydettäessä. Mikäli henkilö toivoo tietojensa toimittamista sähköistä kanavaa pitkin, on rekisteröidyn henkilöllisyys kuitenkin varmistettava ennen toimittamista. Henkilöllisyyden varmistaminen Turun yliopistossa tapahtuu IT-palvelupisteen IT-tukihenkilöiden toimesta, jotka ovat saaneet henkilöllisyyden tarkistamista varten erillisen koulutuksen. Yliopiston palvelupisteellä henkilöllisyyden todentamiseksi hyväksyttyjä henkilötodistuksia ovat Suomen kansalaisten osalta Suomen poliisin myöntämä ajokortti, henkilökortti tai voimassa oleva passi sekä muun kuin Suomen kansalaisten tapauksessa voimassa oleva passi tai Suomen poliisin myöntämä henkilökortti.

5.4 Tietovarasto

Turun yliopistossa on jo vuosia ollut olemassa keskitetty tietovarasto järjestelmien ja rekisterien rajat ylittävän raportoinnin mahdollistamiseksi sekä datan integroimiseksi eri palveluiden käyttöön. Etukäteen ajateltuna katsoin tietovaraston olevan

tutkimukseni hankalin rekisteri tietosuojan näkökulmasta kontaktirekisterin ohella. Henkilörekisterin näkökulmasta tietovarastosta mielenkiintoisen tutkittavan tekee se, ettei se ole oikeastaan minkään henkilötiedon varsinainen lähderekisteri, vaan sisältää ja yhdistelee eri rekistereitä muodostaen näin toki oman erillisen henkilörekisterin. Tästä syystä tietovarasto on käsiteltävä ja huomioitava omana erillisenä tietosuoja-asetuksen alaisena henkilörekisterinä.

Tietovaraston pääasiallinen tehtävä on tuottaa raportteja erilaisista asioista yliopiston sisäiseen sekä Suomen valtion ministeriöiden käyttöön. Pääasiallisesti tietovarastosta tuotettavat raportit ovat täysin anonymisoituja, mikä on hyvä asia tietosuojan näkökulmasta. Tietovarastoa käytetään myös eri palveluiden ja rekisterien tietojen jalostamisena integraatioiden kautta. Myös tiedonsiirroissa Tietovarastoon käytetään pdeudonymisointia, eli henkilöstä siirrossa siirretään vain yksilöivä tunnistetieto ja varsinainen lähdejärjestelmästä tuotava data ja varsinainen yhdistäminen henkilöön tehdään vasta Tietovarastossa itsessään hakemalla tarvittavat täydentävät tiedot Tietovaraston sisäisestä taulurakenteesta.

5.4.1 Palvelun tietoturvallisuus

Tietovarasto sijaitsee Turun yliopiston omassa palvelinympäristössä, yliopiston virtuaalipalvelinalustalle sijoitetulla tietokantapalvelimella. Palvelun tietoturva on toteutettu palvelinkäyttöön tarkoitetulla virustorjunta- ja palomuuriohjelmistolla. Itse palvelimelle käyttöoikeuksia on vain ylläpitohenkilöstöllä. Palvelimelle voi kirjautua vain Turun yliopiston ylläpitoverkosta etätyöpöytäsovelluksella. Palvelimelle kirjaudutaan yliopiston käyttäjätunnuksella ja salasanalla, ja koska koko palvelu on yliopiston IT-henkilöstön itse hallinnoima, ei pääsyä palvelimelle myöskään ole kenelläkään yliopiston ulkopuolisella toimijalla. Tiedonsiirto lähdejärjestelmästä Tietovarastoon tehdään joko suojatulla aineistosiirrolla sftp-protokollaa käyttäen (Secured File Transfer Protocol) sekä Tietovaraston alustaratkaisun omilla integraatiotyöka-

luilla. Näin ollen tiedonsiirto rekisteriin on toteutettu turvallisimmalla mahdollisella tavalla, joka kuitenkin on joustava käyttää.

Koska palvelu sisältää hyvin kriittistä aineistoa yliopiston erilaisista palveluista, osana tutkimustani suosittelen roolipohjaisten käyttöoikeuksien käyttöönottoa palvelussa. Aiemmissa luvuissa kuvatusti 3.1 roolien käyttö luo palvelulle tietoturvallisuutta erityisesti siinä vaiheessa, kun palveluun käyttöoikeudet omaavien henkilöiden työtehtävät muuttuvat syystä tai toisesta. Vaikka ylläpitohenkilöstö on allekirjoittanut asianmukaisesti salassapitosopimuksen, on tietovuodon sattuessa palvelusta vuotaneet tiedot mittavat ja myös haitalliset rekisteröidyille.

Palvelusta toteutettujen raporttien käyttöoikeudet rajataan raporttikohtaisesti. Rajaus perustuu joko yksistään käyttäjän käyttäjätunnukseen, tai vaihtoehtoisesti rajauksessa käytetään tämän lisäksi organisaatiotietoon perustuvaa rajausta, jossa käyttäjällä on oikeus vain oman työsopimuksensa mukaisen organisaatiohaaran dataan. Raporttien käyttöön voi olla oikeus vain Turun yliopiston käyttäjätunnuksella.

5.4.2 Tietovarasto ja rekisterinpitäjän velvollisuudet

Tietovarasto on henkilörekisterinä hieman erilainen luonteeltaan kuin aiemmin tässä tutkielmassani käsittelemät rekisterit. Varsinaisesti tietovarasto ei itsenäisesti sisällä pysyvää henkilörekisteriä, vaan sen sisältämät erilaiset henkilörekisterit ikään kuin luodaan aina uudelleen. Tämä helpottaa luonnollisesti henkilörekisterin ajantasaisuuden ylläpitämistä, mutta hankaloittaa esimerkiksi rekisterinpitäjän näkökulmasta henkilörekisterin luonnetta ja vastuita. Periaatteessa Turun yliopiston IT-palvelut toimivat tietovaraston näkökulmasta henkilötietojen käsittelijän ominaisuudessa, mutta koska itse tietolähteet ovat saman organisaation alaisia, toimii Turun yliopisto rekisterissä joka tapauksessa vain rekisterinpitäjänä. Varsinaisia henkilötietojen käsittelijöitä ei tietovarastossa ole. Henkilörekisterinä tietovarasto ei ole selkeä myöskään henkilötietojen säilyttämisen kannalta, sillä se kokoaa alleen tietoja

henkilörekistereistä, joilla on monta erilaista henkilötietojen säilytysperustetta. Tietovaraston tarkoitus on kuitenkin koota tietoja eri operatiivisista järjestelmistä ja niiden avulla toteuttaa yliopiston toiminnan raportointia ja analysointia. Näin ollen henkilötietojen keräämisen perustana on katsottu olevan Turun yliopiston yleinen etu.

Tietovaraston sisältämän datan arkaluontoisuuden vuoksi koko rekisterin pääsyn rakenne on toteutettu äärimmäisen turvatulla tavalla. Itse tietokantaan pääsyä ei ole kuin tietovaraston pääkäyttäjällä, hänen varahenkilöllään, sekä palvelinylläpitohenkilöillä. Tietovarastopalvelimelle kirjautuminen onnistuu ainoastaan yliopiston IT-palveluiden erikseen eristetystä verkkoympäristöstä, mikä tarkoittaa käytännössä joko IT-palveluiden fyysisistä tiloista tai erillisellä suojatulla VPN-yhteydellä tapahtuvaa käyttöä. Palvelusta tuotettuja raportteja pääsee käyttämään yliopiston utu-tunnuksella. Käyttöoikeudet raportteihin annetaan erikseen ylläpidon toimesta. Tutkimusta tehdessäni havaitsin, että käyttöoikeuksiin liittyi vastaavanlainen uhka tietosuojan näkökulmasta kuin aiemmin tässä tutkimuksessa olen esittänyt opintorekisteriin sisältyneen 5.1.2, eli käyttöoikeudet myönnettiin raportteihin utu-tunnukseen perustuen eikä käyttäjän ja yliopiston väliseen sopimukseen perustuen. Tämä epäkohta palvelusta korjattiin vastaavalla tavalla kuin opintorekisterin tapauksessakin, mutta koska tietovarasto on pysyvä palvelu, suosittelen käyttöoikeuksien toteuttamista paremmin tietosuoja-asetuksen vaatimukset täyttävällä tavalla. Tämä tapa olisi mahdollista ottaa palvelussa käyttöön nykyisen identiteetinhallintajärjestelmän kautta varsin helposti. Käyttöoikeuksia tietovarastosta tuotettaviin raportteihin anotaan rekisterin ylläpitäjiltä, jotka varmistavat käyttäjäorganisaation pääkäyttäjiltä erikseen luvan oikeuksien myöntämiseen ennen käyttöoikeuden antamista. Usein pyyntö käyttöoikeuksien lisäämiselle tulee jo suoraan pääkäyttäjältä. Lisäksi raporttikohtaisesti rajauksia on mahdollista tehdä käyttäjän työsopimuksen kustannuspaikkaan liittyen niin, että henkilöllä ei ole mahdollista saada tietyn toi-

mialan raportteihin oikeuksia ilman, että hänellä on kyseiseen toimialaan liittyvä sopimus olemassa. Mielestäni tämä rajauksen mahdollisuus on erinomainen seikka käyttöoikeuksissa tietosuojan näkökulmasta. Tietovaraston käyttöä lokitetaan palvelimelle kirjautumisten osalta asianmukaisesti, mutta raporttien tarkastelu palvelussa on jätetty lokituksen ulkopuolelle. Raportille kirjautumiset kerätään lokille kyllä, mutta itse hakutulokset eivät lokitietoon päädy. Näin ollen palvelu ei aivan täysin täytä tietosuoja-asetuksen asettamia vaatimuksia, sillä henkilötietojen käsittely rekisteröidyn tietojen katselun osalta ei ole selvitettävissä. Yksi vaihtoehtoinen toteutus lokituksen kehittämiseksi olisi vastaava kuin yliopiston kontaktirekisterissä toteutettu, eli suoritettujen hakulausekkeiden rekisteröinti lokiin. Näin datan hakutulokset olisi toistettavissa jälkikäteen, tosin muuntuneella datalla, mutta monasti jo tämäkin voisi sulkea pois tai antaa olettaa henkilön tietojen olleen tarkastelun alla tai jääneen tarkastelun ulkopuolelle. Tämäkään ei täydellisesti täyttäisi siis Tietosuoja-asetuksen lokitukselle asettamia vaatimuksia, mutta olisi kuitenkin parempi kuin nykyinen käytäntö.

Kuitenkin on huomioitava, että tietovarastosta tuotetut raportit ovat pääasiassa täysin anonymisoituja joitakin erityistarpeita varten tuotettuja raportteja lukuun ottamatta. Näin toimien on myös saatu lähes kokonaan poistettua mahdollisuus henkilötietojen päätymisestä sellaisten tahojen haltuun, joilla ei niihin ole oikeutta. Koska tämä anonymisointi ei kuitenkaan ole täysin kattava, on edellä esitetyt parannukset tietovaraston käyttöoikeuksien hallinnan parantamiseksi syytä ottaa joka tapauksessa harkintaan.

Tietovarastoon kerätään dataa metatietojärjestelmistä aina tiettyä tarvetta varten. Tarve voi olla raportti tai dataa voidaan vaatia, jotta jokin toinen data saataisiin luotettavasti muodostettua. Kutakin tarvetta varten datan määrä pyritään joka kerta minimoimaan, jotta tietovaraston koko pystytään pitämään mahdollisimman pienenä. Näin lähtökohtaisesti myös henkilötietojen ollessa kyseessä, ei tietovaras-

toon tuoda yhtään enempää henkilötietoja, kuin tarvetta varten on välttämätöntä. Henkilötietojen päivittymisen suhteen tietovarasto on aina riippuvainen metadata-rekisteristä, sillä tietovaraston aineistot koostuvat vain niistä tuotetuista tiedoista. Jos siis henkilötieto on päivittynyt metatietojärjestelmässä tai -rekisterissä, päivtyy se myös tietovarastossa. Sama koskee myös henkilötietojen poistumista rekisteristä; myös sen suhteen tietovarasto on täysin riippuvainen metatietorekisteristä. Kun henkilötieto poistuu lähdejärjestelmästä arkistointivelvoitteen päätyttyä tai muusta syystä, ei tieto välity enää myöskään tietovarastoon ja näin tieto poistuu rekisteristä.

Tietovarastoon ei ole tehty erikseen mahdollisuutta rekisteröidyn henkilötietojen saamiseksi ulos palvelusta rekisteröidyn tarkastelua varten, sillä koko tietovaraston raportointi ja muu käyttö perustuu tietojen kokoamiseen eri tietovaraston tauluja yhdistäen. Näin myös tietyn henkilön pyytämät henkilötiedot on mahdollista tuottaa tietovarastosta tarpeen mukaiseen taulujoukkoon ulottuvan SQL-kyselyn avulla pääkäyttäjien toimesta.

5.4.3 Tietovarasto ja rekisteröidyn oikeudet

Koska tietovaraston henkilötiedot koostetaan lähdejärjestelmistä tuotettavien tietojen pohjalta, ei henkilön unohtaminen rekisteristä ole käytännössä mahdollista. Henkilötietojen poistaminen tulee käytännössä tapahtua lähdejärjestelmään, jolloin tiedot poistuvat automaattisesti myös tietovaraston datasisällöstä.

Tietovarastosta henkilörekisterinä on kirjoitettu Tietosuoja-asetuksen mukainen tietosuojailmoitus. Tätä ilmoitusta ei kuitenkaan ole saatavissa yliopiston julkisten verkkosivujen kautta, minkä näen pienimuotoisena puutteena. Koska tietovarasto ei ole mukana myöskään yliopiston julkaisemalla tietopyyntölomakkeella, ei rekisteröidyllä ole käytännössä edes tietoa hänen henkilötietojensa sijaitsemisesta tietovarastossa. Tietovaraston luonteen vuoksi tämä on periaatteessa hyväksyttävää, mut-

tei mielestäni täytä täysin niitä avoimuuden periaatteita, joita tietosuoja-asetus on laadittu valvomaan ja noudattamaan. Kuitenkin jokaisen tietovaraston käyttämän lähdejärjestelmän tietosuojailmoituksessa tulisi olla maininta tietovarastosta henkilötietojen vastaanottajana, joten sen kautta rekisteröidyn on mahdollista saada tieto henkilötietojensa päätymisestä tietovarastoon. Kuitenkin syy henkilötietojen viennistä tietovarastoon saattaa jäädä tällöin epäselväksi rekisteröidylle.

5.5 Yhteenveto havainnoista

Tässä luvussa kävin läpi tutkimukseen valitut Turun yliopiston ydintoiminnan kannalta merkittävät henkilörekisterit ja arvioin jokaisen rekisterin kohdalla myös yliopiston kykyä noudattaa toimintaperiaatteita, jotka kuvasin luvun neljä aliluvussa 4.12 4.12. Kokonaisuutena voin sanoa Turun yliopiston tilanteen rekisterien suhteen olevan hyvä, vaikka jokaisesta henkilörekisteristä löytyikin kehityskohteita ja korjattavia seikkoja. Turun yliopisto täyttää Tietosuoja-asetuksen rekisterinpitäjälle määrittämät velvollisuudet suurimmalta osin. Kahden rekisterin (henkilöstörekisteri ja tietovarasto) käyttäjähallinta tapahtui manuaalisesti myönnettävillä oikeuksilla ja näiden osalta esitinkin analyysissäni korjaustoimet asian kuntoon saattamiseksi. Suurin puute henkilöstörekistereissä oli henkilötietojen käsittelytoimien lokitus, mikä on rekisterien käyttölaajuuden ja rekisterin koon vuoksi jopa ymmärrettävää. Myös rekisteröidyn mahdollisuudessa saada itseä koskevat tiedot henkilörekistereistä oli tutkimuksen kohteena olevista rekistereistä puolessa (Opsu ja tietovarasto) mahdotonta, mutta näissäkin organisaatiolla on kyvykkyys tieto rekisteristä erikseen kerätä, joten en näe tätä rekisterien suhteen merkittävänä puutteena. Positiivisena pidän sitä, että jo henkilörekisterien analysoinnin aikana havaittuihin puutteisiin ja poikkeamiin reagoitiin organisaatiossa viipymättä ja havaitut poikkeamat saatettiin kuntoon.

6 Yhteenveto tutkielmasta

6.1 Tutkielman tavoitteet ja opit

Tämän tutkielman tarkoituksena oli selvittää ja tutkia Turun yliopiston merkittävimpien henkilörekisterien valmiutta vastata Tietosuoja-asetuksen rekistereille asettamiin haasteisiin sekä tutkia yliopiston tapaa käsitellä henkilötietoja tietosuojan näkökulmasta. Tutkimuskysymyksiksi työlle asetin:

- Tutkimuskysymys 1: Miten tarkastella ison organisaation GDPR:n mukaisuutta?
- Tutkimuskysymys 2: Mitä voidaan todeta Turun yliopiston keskeisten rekisterien tietosuoja-asetuksen mukaisuudesta?

Ensimmäisen tutkimuskysymyksen asettelun haasteellisuuden ymmärsi tarkasteltujen rekisterien kautta hyvin, vaikka itse tutkimuskysymys olikin juuri oikeaan ja haluttuun tarpeeseen tähtäävä. Tutkielmani ja läpikäymieni rekisterien kautta sain hyvän käsityksen koko organisaation yleisestä valmiudesta käsitellä henkilötietoja ja henkilörekistereitä Tietosuoja-asetuksen vaatimalla tavalla. Mutta toisaalta taas sen ja Tietosuoja-asetuksen kokonaisuuden sisäistämällä ymmärsin myös sen, ettei yksittäisten henkilörekisterien tutkiminen anna vielä tulosta koko organisaation valmiustasosta. Jokainen henkilörekisteri on oma kokonaisuutensa eikä erinomaisesti hoidettu henkilötietojen käsittely niissä kerro vielä koko totuutta organisaatioiden muista henkilörekistereistä tai henkilötietojen käsittelyn tilasta niiden suhteen.

Mutta hyvän olettamuksen tätä tutkimus antaa, sillä jos perusasiat hoidetaan hyvin näiden rekisterien osalta, ovat perusasiat yhtälailla kunnossa muidenkin henkilörekisterien suhteen.

Yllä kuvattu pohdinta antaakin vastauksen tutkielman toiseen tutkimuskysymykseeni, eli yhteenvetona voin todeta, että Turun yliopistossa on tehty hyvin pohjatyö henkilötietojen käsittelystä esimerkiksi palvelinarkkitehtuurin, kirjautumiskäytäntöjen, identiteetinhallinnan ja organisaation yleisen valveutuneisuuden suhteen. Mutta isossa, julkisoikeudellisessa organisaatiossa henkilörekisterien kirjo on niin valtava, että kattavaa toteamusta koko organisaation tietosuoja-asetuksen mukaisuudesta on mahdotonta tehdä ilman, että kävisi läpi kaikki organisaatiossa olevat henkilörekisterit.

Tutkielmani koostaminen vei liikaa aikaa siihen nähden, mikä tarve Turun yliopistolla olisi ollut saada työn tulokset käyttöönsä. Toisaalta itse rekisterien valmiuden tarkastelu tutkielmaa tehdessä tehtiin ajoissa Tietosuoja-asetuksen voimaantuloon mennessä, mutta tulosten raportoiminen valmiin tutkielman muodossa vei liikaa aikaa. Itse tutkimusmenetelmänä katson toimineeni täysin oikein, eli ensisijaisesti sisäistäen Tietosuoja-asetuksen sisällön ja sen jälkeen peilaten oppimaani itse henkilörekistereihin. Ajallisesti koko maailma on ehtinyt tietosuojan näkökulmasta muuttua paljon Tietosuoja-asetuksen voimaantulon jälkeen ja mielikuva tietosuojan huomioimisesta ja vaatimuksista on ehtinyt muuttua sen myötä, joten sen myötä myös näkemykseni yliopiston toimintatavoista ovat myös selkeytyneet. Turun yliopistossa työskentelytavat hyvien henkilötietojen käsittelyn eteen oli aloitettu jo paljon ennen varsinaista valmistautumista Tietosuoja-asetuksen voimaan tuloon. Tämä hyvä pohjatyö loi myös hyvät edellytykset yksittäisten henkilörekisterien tarkastelulle, jota yliopistossa tehtiin hyvin koordinoidusti. Kun Tietosuoja-asetus astui voimaan, oli yliopisto saanut tietosuojatyön henkilörekisterien suhteen kutakuinkin valmiiksi ja kokonaiskuva yliopiston henkilörekisterien tilasta oli hyvä. Valitettavasti kuiten-

kin tietosuojatyön ponnistelujen tuoima väsymys näkyi organisaatiossa siten, ettei työn aikana havaittuja puutteita ja tietosuojatyön käytäntöjä enää edistetty intensiivisesti organisaatiossa ja ponnistelut hyvän tietosuojan edistämiseksi loppuivat. Työni yhteenvetona voin todeta, että edelleen Turun yliopistolla on todella hyvät valmiudet tehdä koko organisaation laajuudella erinomaista henkilötietojen käsittelyä, mutta käytänteet, prosessit ja suunnitelmallisuus työn edistämiseksi on luotava ja otettava käyttöön koko organisaatiossa.

Yhteenvetona Tietosuoja-asetuksesta ja sen mukanaan tuomasta henkilörekisterien tietosuojasta voin sanoa, että itse asetus oli todella merkittävä virstanpylväs koko maailmalle ja toi mukanaan täysin uuden tavan ajatella henkilötietoja ja niiden haavoittuneisuutta. Tietosuoja-asetus näyttäytyi monelle täysin turhana valvomisena, koska suuri osa ihmisistä ei ymmärrä eikä ole sisäistänyt henkilörekisterien sisältämää riskia ihmiselle. Mutta palveluiden tietoturvan ja henkilötietojen turvaamisen näkökulmasta Tietosuoja-asetus toi mukanaan täysin uuden toimintatapakulttuurin ja tavan ajatella henkilötietojen turvaamisen tarvetta ja ihmisistä säilöttävien henkilötietojen haavoittuvuutta. Tietosuoja-asetus käänsi yhteiskunnalle täysin uuden sivun henkilötietojen käsittelyssä ja aloitti tietosuojan näkökulmasta täysin uuden aikakauden.

Lähdeluettelo

[1] *Turun yliopiston Vuosikertomus 2021: Hyvinvoiva yhteisö [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/yliopisto/vuosikertomus-2021/hyvinvoiva-yhteiso.

[2] *Turun yliopiston Vuosikertomus 2021: Koulutus [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/yliopisto/vuosikertomus-2021/koulutus.

[3] *Euroopan parlamentin ja neuvoston asetus EU 2016/679. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). [Online.] Saatavissa:* https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[4] *Turun yliopiston johtosääntö 2021 [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/sites/default/files/public%3A/media/file/turun-yliopiston-johtosaanto.pdf.

[5] *Yliopistolaki. [Online.] Saatavissa:* https://www.finlex.fi/fi/laki/ajantasa/2009/20090558.

[6] *Henkilörekisterilaki. [Online.] Saatavissa:* https://www.finlex.fi/fi/laki/alkup/1987/19870471.

[7] *Arkistolaki. [Online.] Saatavissa:* https://www.finlex.fi/fi/laki/ajantasa/1994/19940831.

[8] *Erillisopinnot. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/opiskelijaksi/erillisopinnot.

[9] *Tietosuojailmoitus - opiskelijoiden henkilötietojen käsittely koulutuksen yhteydessä. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/tietosuoja/tietosuojailmoitus/opiskelijoiden-henkilotiedot.

[10] *Tietosuojailmoitus / Turun yliopiston henkilöstörekisteri. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/sites/default/files/public%3A//media/file/Tietosuojailmoitus%20HR%20j%C3%A4rjestelm%C3%A4t%206.2020.pdf.

[11] *Alumniksi rekisteröityminen Turun yliopistosta ja Turun kauppakorkeakoulusta valmistuneille. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://konsta.utu.fi/en-us/Julkinen-eTapahtuma-ps/Alumnitietojen-paivitys.

[12] *UTU-käyttäjätunnus ja salasana. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/yliopisto/langattomat-verkot-kayttajatunnukset-ja-it-tuki/utu-kayttajatunnus-ja-salasana.

[13] *Kontaktien ja tapahtumien hallintajärjestelmän tietosuojailmoitus. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/tietosuoja/tietosuojailmoitus/konsta.

[14] *Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. [Online.] Saatavissa:* https://eur-lex.europa.eu/legal-content/FI/TXT/HTML /?uri=CELEX:31995L0046&from=FI.

[15] *Tietosuojavaltuutetun toimisto. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://tietosuoja.fi/tietosuojavaltuutetun-toimisto.

[16] *Tietosuojaperiaatteet. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://tietosuoja.fi/tietosuojaperiaatteet.

[17] *Data Security description of University of Turku. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/en/privacy/data-security-description.

[18] *IT-palvelujen käyttösäännöt. [Online.][Viitattu 9.6.2022.] Saatavissa:* https://www.utu.fi/fi/yliopisto/langattomat-verkot-kayttajatunnukset-ja-it-tuki/utu-kayttajatunnus-ja-salasana/kayttosaannot.

[19] *Laki viranomaisten toiminnan julkisuudesta. Saatavissa:* https://www.finlex.fi/fi/laki/ajantasa /1999/19990621.

[20] *Työsopimuslaki. [Online.] Saatavissa:* https://www.finlex.fi/fi/laki/ajantasa /2001/20010055.