Esko Rikkonen

EU:n tietosuoja-asetus 2016/679 (GDPR) ohjelmistoyrityksessä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

30.11.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Esko Rikkonen EU:n tietosuoja-asetus 2016/679 (GDPR) ohjelmistoyrityksessä 30 sivua 30.11.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Ohjelmistotekniikka
Ohjaaja(t)	Lehtori Juha Kämäri Teknologia-arkkitehti Mika Kukkonen

Insinöörityössä tavoitteena oli tutustua EU:n tietosuoja-asetukseen 2016/679 sekä selvittää, millaisia vaatimuksia se aiheuttaa työn tilanneessa ohjelmistoyrityksessä ja suunnitella ja toteuttaa osa muutostöistä. Työn tavoitteet suunniteltiin yhdessä tilaajayrityksen kanssa.

Työn aikana selvitettiin tietosuoja-asetuksen sisältöä ja sitä, miltä osin se kohdistuu yritykseen ja kuinka asetuksen ehdot käytännössä toteutettaisiin. Selvityksen aikana pyrittiin muodostamaan selkeä kuva siitä, missä asetuksen määrittämissä rooleissa yritys toimii ja mitkä niistä muodostuvat vastuut ovat. Pyrittiin myös muodostamaan käsitys yrityksen asiakkaiden tulevista tarpeista, joiden perusteella yrityksen ohjelmistotuote voitaisiin valmistella vastaamaan asetuksen vaatimuksia.

Selvityksen perusteella yritykselle tehtiin nykytila-analyysi, jolla pyrittiin dokumentoimaan yrityksen tietoturvakäytännöt ja määrittämään, mitä puutteita yrityksen hallinnollisissa ja teknisissä tietoturva ja -suojakäytännöissä on. Analyysin perusteella priorisoitiin kehitysprojekteja yrityksen toimintatapojen ja ohjelmistotuotteen parantamiseen.

Työn tuloksena luotiin uusia ominaisuuksia työn tilaajan ohjelmistotuotteeseen. Näitä olivat rekisteröityjen suostumuksen pyyntö ja tiedotus heidän oikeuksistaan, oikeus tulla unohdetuksi ja tietojen siirto. Lisäksi tarkastettiin ja laajennettiin tilaajayrityksen tietoturvasuunnitelmaa, tietoturvaesitettä ja tietoturvaohjeistusta yrityksen henkilöstölle ja asiakkaille.

Avainsanat	EU, tietosuoja-asetus, 2016/679, GDPR, tietosuoja, tietoturva

Author(s) Title Number of Pages Date	Esko Rikkonen General data protection regulation 2016/679 at a software company 30 pages 30 November 2017
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Software engineering
Instructor(s)	Juha Kämäri, Senior Lecturer Mika Kukkonen, Technology Architect

Aim of this thesis was to get acquainted with EU data protection regulation 2016/679, find out which of its requirements are notable in a software company that ordered the thesis and implement a part of the changes needed. Goals of the thesis were planned together with the company.

Contents of the Data protection regulation were studied and a viewed from the roles the company is in as a data controller and a data processor. Company's clients were studied to predict what requirements they will have for the company's main software product soon.

Based on the theoretical study, a current state analysis was done to document company's managerial and technical data protection practices and find their flaws. Based on the analysis a few development projects were formed and prioritized especially focusing on the company's main software product.

Thesis' results were data protection documentation and guidelines for the company's personnel and clients and software feature implementations which enable data subjects' rights to be forgotten, to transfer their data and to gather their consent and inform them of their rights.

Keywords	GDPR, EU, 2016/679, data protection, data security

Sisällys

Lyhenteet

1 Johdanto 1

2 Lähtökohdat 1

2.1 Osapuolet: Rekisteröity, rekisterinpitäjä ja käsittelijä 3
2.2 Henkilötiedon ja käsittelyn määritelmä 3
2.3 Henkilötietojen elinkaari 4
2.4 Muutokset aikaisempaan lainsäädäntöön 5
2.5 Rekisteröidyn oikeudet 5
2.6 Rekisterinpitäjän velvollisuudet 7
2.6.1 Oikeusperusta 7
2.6.2 Oletusarvoinen tietosuoja 8
2.6.3 Tietoturvan hallinta 8
2.6.4 Tiedonanto ja yhteistyövelvoite 10
2.6.5 Tiedonsiirto Euroopan talousalueen ulkopuolelle 11
2.7 Käsittelijän velvollisuudet 12
2.8 Vastuunjako ja sopimukset 13

3 Valmistautuminen ohjelmistopalveluyrityksessä 14

3.1 Nykytila-analyysi 14
3.2 Tietoturvan dokumentointi 17
3.3 Jatkotoimenpiteet 19

4 Ohjelmistotuotteen muutokset 20

4.1 Tuotteen yleiskuvaus 20
4.2 Asiakkaiden erojen huomiointi 21
4.3 Suostumuksen pyyntö 22
4.4 Tietojen siirto 24
4.5 Oikeus tulla unohdetuksi 26

5 Yhteenveto 29

Lähteet 31

Lyhenteet ja käsitteet

Artikla	EU:n asetuksen yksittäinen pykälä.
Asetus	EU:n asettama pakottava lainsäädäntö joka tarvittaessa kumoaa jäsenmaissa olevat päällekkäiset lait.
ASP.NET	Verkkosovellusten kehittämiseen tarkoitettu ohjelmistokirjasto.
Direktiivi	EU:n antama lainsäädäntäohje, joka toteutetaan erikseen kunkin jäsenmaan lainsäädännössä.
DNN	DotNetNuke. Sisällönhallinta ja verkkojulkaisujärjestelmä.
EU	Euroopan unioni.
GDPR	General Data Protection Regulation. EU:n asetus 2016/679 luonnollisen henkilön oikeuksista tietojensa rekisteröinnin suhteen.
Henkilötieto	Tunnistettavissa olevaan luonnolliseen henkilöön liittyvää tietoa.
JSON	Javascript object notation. Tiedonsiirtomuoto.
Käsittelijä	GDPR:ssä määritelty henkilötietojen käsittelyä rekisterinpitäjän toimesta tekevä taho.
Rekisteröity	Luonnollinen henkilö, jonka henkilötietoja käsitellään.
Rekisterinpitäjä	Henkilötietorekisterin omistaja.
REST	Representational state transfer. Tekniikka yhdistää verkkopalveluita.
SQL	Structured query language. Relaatiotietokannoille suunnitelu kyselykieli.
XML	Extensible markup language. Kieli jolla määritellään rakenteellisia kuvauskieliä.

1 Johdanto

Euroopan unioni hyväksyi 27.4.2016 kansallisia tietosuojalainsäädäntöjä yhtenäistävän tietosuoja-asetuksen 2016/679. Asetus määrää aikaisempaa laajemmin henkilörekisterien pitäjiin ja käsittelijöihin kohdistuvia vastuita ja velvollisuuksia sekä rekisteröidyn oikeuksia. Asetus on jo voimassa. Sen noudattamiselle on kuitenkin annettu siirtymäaika, joka päättyy 28.5.2018. Tietotekniikkayritykset, jotka eivät siihen mennessä saa toimintaansa osoitettavasti asetuksen tasolle, kokevat tuntuvan kolahduksen kilpailukyvyssään ja omassa toiminnassaan asiakkaiden alkaessa vaatia asetuksen vaatimusten täyttävää toimintaa.

Insinöörityön tilaaja on pieni ohjelmistoyritys. Sen pääliiketoiminta on henkilötietoja käsittelevän HR-ohjelmistotuotteen kehitys ja ohjelmistopalveluiden tarjonta. Yritys toimii henkilötietojen käsittelijänä lähes kaikille asiakkailleen. Liiketoiminnan jatkumiseksi on kriittistä osoittaa riittävä tietoturvakäytäntöjen taso sekä yrityksen toiminnassa, teknisissä ympäristöissä että sen pääohjelmistotuotteen tietoturvan tasossa. Tämä on tehtävä sekä asiakkaiden luottamuksen säilyttämiseksi että lainsäädännöllisten velvollisuuksien vuoksi.

Työn tavoitteena on kartoittaa tilaajayrityksen tietoturvakäytäntöjen ja ohjelmistotuotteen tietoturvan nykytila, laatia suunnitelma havaittujen EU:n tietosuoja-asetuksen vaatimuksiin verrattuna esiintyvien puutteiden korjaamiseen sekä toteuttaa ohjelmistoon oleellisimmat asetuksen vaatimuksia tukevat ominaisuudet.

2 Lähtökohdat

Euroopan parlamentti ja neuvosto säätivät 27.4.2016 asetuksen, joka säätelee luonnollisten henkilöiden tietosuojaa koko Euroopan unionin alueella. Asetuksesta käytetään nimeä General Data Protection Regulation (GDPR). Asetus astui voimaan jo vuoden 2016 toukokuussa, mutta sitä aletaan soveltamaan kahden vuoden siirtymäajan jälkeen 28.5.2018.

Asetuksen on tarkoitus yhtenäistää eri maiden henkilötietolainsäädäntöä. Erityisesti säädös vahvistaa yksityishenkilöiden asemaa tietojenkäsittelyssä ja määrittää henkilötietoja

käsitteleville organisaatioille vastuita ja velvollisuuksia. Valtiovarainministeriön julkaisemassa VAHTI-raportissa 1/2016 [2016: 5] painotetaan digitalisaation ja uusien teknologioiden ja palvelutapojen kasvun luomaa tarvetta henkilötietojen kattavammalle hyödyntämiselle ja tarvetta saattaa henkilötietolainsäädäntö tämän uuden, myös yleisöllä entistä keskeisemmän, tietosuojakulttuurin tasolle. Liiketoimintaympäristön kehittäminen vaati tasapainoa yksilön suojan ja liiketoiminnan mahdollistamisen välillä. Tietosuoja-asetuksessa 2016/679 [2016: 2] motiiveiksi mainitaankin esimerkiksi tietojen kansainvälisen liikkuvuuden ja lainsäädännöllisen selkeyden parantaminen: Päättäjät haluavat kasvattaa luottamusta henkilötietojen käsittelyyn.

Asetus antaa myös mahdollisuuden määrätä tuntuvat sakot tietosuojaa laiminlyöville organisaatioille [Asetus 2016/679 2016: 83]. Organisaatiot ovat paitsi velvollisia huolehtimaan tietoturvasta myös osoittamaan, että henkilötietojen käsittely tehdään tietoturvallisesti: Valvontaviranomaisella on oikeus auditoida organisaatioiden tietoturvaa [VAHTI-raportti 1/2016: 30].

Ohjelmistoyrityksen arkea tietosuoja-asetus koskee paitsi silloin kun yritys toimii itse rekisterinpitäjänä, niin myös sen tuottaessa palveluita tai tuotteita, joilla henkilötietoja käsitellään. Hankkijat joutuvat huomioimaan tietoturvavaatimukset entistä tarkemmin jo tarjousvaiheessa, ja yritysten kannattaakin varautua tarjoamaan selontekoa hallinnollisista ja teknisistä tietoturvaratkaisuistaan potentiaalisille asiakkaille. Myös tietoturva-auditointeja tullaan varmasti tekemään entistä useammin.

Rahanmenoa aiheuttaa myös esimerkiksi tietojenkäsittelyn todistettavaan seurattavuuteen ja tietosuojavastaavan työhön liittyvät kustannukset. Jo Suomen aiemman henkilötietolain puitteissa ylläpidettiin rekisteriselosteita, mutta tietosuoja-asetuksen myötä rekisterinpitäjät ja käsittelijät joutuvat dokumentoimaan käsittelytoimensa. Monessa tietosuojaan vakavasti suhtautuneessa organisaatiossa uuden lainsäädännön aiheuttamat työt ovat vähäisempiä, mutta tulee olemaan myös paljon yrityksiä, jotka eivät ole ehtineet varautumaan tietosuoja-asetuksen aiheuttamiin vaatimuksiin. IT-tutkimus ja -konsultointiyritys Gartner arvioi keväällä 2017, että yli 50 % yrityksistä ei ole täysin asetuksen mukaisia [Forni & van der Meulen 2017] siirtymäajan päättyessä 2018.

Asetuksenmukaisuuden toteuttaminen organisaatiossa vaatii sekä hallinnollisia menetelmiä että tietojenkäsittelyjärjestelmien kehitystä. Henkilötietojen kohteiden oikeuksien toteuttaminen kustannustehokkaasti ja oletusarvoisen tietoturvan syntyminen vaativat,

että ne on ohjelmistoissa huomioitu. Asetus esittää suoria vaatimuksia rekisterinpitäjien organisaatioiden ja dokumentaation osalta.

2.1 Osapuolet: Rekisteröity, rekisterinpitäjä ja käsittelijä

Asetus määrittelee kolme keskeistä roolia. Asetus rakentuu näiden roolien keskinäisten suhteiden ja oikeuksien ja vastuiden ympärille. Lisäksi asetus määrittelee valvontaviranomaisien toimintaa tarkentavia säädöksiä. Vahti-raportti 1/2016 [2016: 37] määrittelee eri termit selkeästi:

Rekisteröity (data subject) on luonnollinen henkilö, jonka henkilötietoja käsitellään. Asetuksessa on erityisiä vaatimuksia alaikäisten rekisteröityjen huomioimiseen.

Rekisterinpitäjä (data controller) on taho, joka määrittelee käsittelyn tarkoitukset ja keinot. Se on luonnollinen henkilö tai oikeushenkilö tai julkishallinnon elin, jonka päätöksestä henkilötietoja käsitellään. Rekisterinpitäjä määrittelee käsittelyn perusteet ja keinot ja on ensisijaisesti vastuussa käsittelystä.

Käsittelijä (data processor) on henkilötietoja rekisterinpitäjän toimeksiannosta käsittelevä taho. Käsittelijän tekee töitä rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Sillä on kuitenkin oikeudellinen vastuu: Käsittelijän tulee itse varmistua, että käsittely vastaa EU:n tai jäsenvaltion lainsäädännön ehtoja.

Käsittelijästä voi tulla rekisterinpitäjä, jos se itse määrittää käsittelyn tarkoituksia tai keinoja [Asetus 2016/679 2016: 50]. Käsittelyä tekevän yrityksen kannattaa varmistua siitä, että kaikki sen tekemät käsittelytoimenpiteet on yksilöity kirjallisissa sopimuksissa. Muutoin se voi yllättäen joutua aikomaansa vastuullisempaan asemaan rekisterinpitäjänä.

2.2 Henkilötiedon ja käsittelyn määritelmä

Tietosuoja-asetus koskee vain henkilötietoja. Asetuksen 2016/679 4 artiklassa [2016: 33] määritellään, mitä ne tarkalleen ovat:

> Kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön […] liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilö-

> tunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

On siis hyvä huomata, että kun henkilötietojen käsittely lopetetaan syystä tai toisesta, data voidaan poistamisen sijaan esimerkiksi anonymisoida poistamalla tunnistetiedot. Tällöin kaikkea henkilöön liittyvää muuta tietoa ei tarvitse poistaa kokonaan.

Toinen tietosuoja-asetuksen keskeinen määritelmä on ’käsittely’. Sillä tarkoitetaan

> tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Käsittelyä on siis kaikki tietoihin liittyvä toiminta, myös niiden säilytys ja poistaminen. Täten kun henkilötietoja on kerätty, voi lainsäädäntö myös rajoittaa niiden poistamista. Samoin asetuksen määräysvalta ulottuu esimerkiksi varmuuskopioihin, mikä aiheuttaa mielenkiintoisia asioita esimerkiksi rekisteröidyn oikeuden tulla unohdetuksi.

2.3 Henkilötietojen elinkaari

Tietosuoja-asetuksen 2016/679 5 artikla [2016: 35] "Henkilötietojen käsittelyä koskevat periaatteet" linjaa tietojen keräykseen, käytön ja säilytyksen perussäännöt. Rekisterinpitäjän tulee määritellä ja tiedottaa selkeästi, mihin tarkoitukseen tiedot kerätään, eli toteutuu "käyttötarkoitussidonnaisuus". Tietoja ei saa hyödyntää muihin käyttötarkoituksiin. Tästä poikkeuksen muodostavat esimerkiksi tilastolliset ja tieteelliset tarkoitukset. Kerättävät tiedot on rajoitettava käyttötarkoituksen kannalta oleellisiin. Asetus kutsuu tätä "tietojen minimoinniksi".

Käsittelyn jatkuessa rekisterinpitäjän on kohtuullisin toimenpitein pyrittävä pitämään tiedot "täsmällisinä" eli ajantasaisina ja poistaa tai oikaista virheelliset henkilötiedot. Tässäkin artiklassa asetus toistaa vaatimuksen tietojen "eheyden ja luottamuksellisuuden" säilymisestä: Tietoja on suojeltava mahdollisuuksien mukaan sekä väärinkäytöltä että vahingoilta.

Henkilötiedot tulee poistaa, kun tietoja ei enää tarvita toden käsittelytarkoituksen toteuttamisessa. Vaihtoehtoisesti tiedot voi anonymisoida, eli muuttaa siten, ettei rekisteröityä voi niistä enää tunnistaa. Vahti-raportin 1/2016 mukaan [2016: 24], jos tietojen poiston

estää esimerkiksi jokin toinen säädöksellinen este, niin ne on arkistoitava sopivalla tavalla, että niiden muu käsittely rajoittuu. Raportti myös tähdentää, että tietojen poisto on huomioitava jotenkin, että ne eivät palaudu käsittelyyn esimerkiksi muun ongelmatilanteen jälkeen tietojärjestelmän varmuuskopiota palautettaessa. Tästä asetus käyttää termiä "säilytyksen rajoittaminen".

Rekisterinpitäjällä on osoitusvelvollisuus näiden asioiden suhteen, eli sen pitää pystyä osoittamaan, että nämä ehdot toteutuvat [Asetus 2016/679 2016: 36]. Se voidaan tehdä esimerkiksi laatimalla organisaatiolle tietotilinpäätös. Tietotilinpäätös on vapaamuotoinen raportti, joka pyrkii tarjoamaan kokonaiskuvan organisaatiossa tapahtuvasta tietojenkäsittelystä: Mitä tietoja käsitellään, kenen toimesta ja millä tavoin.

2.4 Muutokset aikaisempaan lainsäädäntöön

Asetus korvaa EU-direktiivin 95/46/EY, johon Suomen nykyinen henkilötietolaki pohjautuu [Nevala 2017]. Asetus seuraa direktiiviä monilta osin laajentaen ja tarkentaen sen määritelmiä.

Chaturvedi [2017] käy artikkelissaan Comparison of General Data Protection Regulation and Data Protection Directive läpi keskeiset erot aiempaan direktiiviin. Rekisteröidyn oikeuksia on monelta osin kasvatettu. Esimerkiksi tiedonsaantioikeutta ja pääsyä tietoihin on parannettu, samoin kuin tietojen poistamisen pyytämiseen liittyviä sääntöjä. Tosin samalla on myös tarkennettu esimerkiksi perusteita, joiden varassa rekisterinpitäjä voi kieltäytyä lopettamasta tietojen käsittelyä. GDPR myös määrittelee, miten tietojen kohteelta pitää pyytää suostumus tietojen käsittelyyn yleisesti ja erityisesti lasten tapauksessa.

Kokonaan uusia organisaatioiden velvollisuuksia ovat Chaturvedin mukaan muun muassa tietosuojavastaavan nimitys ja erilaiset tietoturvan todentamiseen liittyvät velvoitteet kuten tietosuojan vaikutustenarvioinnit, jos käsittelyyn liittyy erityisiä riskejä. Toimijat joutuvat myös pitämään kirjaa käsittelytoimista.

2.5 Rekisteröidyn oikeudet

Luonnollisten henkilöiden tietojen suojeleminen ja yksilön oikeudet ovat tietoturva-asetuksen keskiössä. Henkilötietojen käsittelyyn pitää aina olla laillinen peruste tai kohteen

suostumus. Asetus määrittelee tarkkaan, että suostumus on pyydettävä yksiselitteisesti ja painostamatta. Enää ei riitä valmiiksi täytetty rasti ruutuun rekisteröitymislomakkeen lopussa. Jos kyseessä on alle 13-16 vuotias rekisteröity, niin suostumus on saatava hänen huoltajaltaan. Tarkka ikä määräytyy kunkin jäsenmaan lainsäädännössä [Asetus 2016/679 2016: 37].

Asetus määrää useita tapoja joilla henkilötietojen kohteiden pitää päästä käsiksi häntä koskeviin tietoihin [VAHTI-raportti 1/2016: 14]. Henkilöllä on oikeus saada pyynnöstä omat tietonsa tarkasteltavaksi sekä vaatia tietojen korjaamista tarvittaessa. Samoin rekisteröity voi pyytää tietojensa siirtämistä rekisterinpitäjältä toiselle [VAHTI-raportti 1/2016: 16]. Käytännössä tämä tarkoittaa vähintään, että tiedot on saatava ulos jossain jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa kuten XML- tai JSON-tiedostona.

Henkilöillä on myös tiedonsaantioikeus. Vahti-raportti 1/2016 [2016: 14] luettelee asiat, joita rekisterinpitäjän tulee tiedottaa rekisteröidylle. Monet niistä olivat jo henkilötietolaissa, esimerkiksi rekisterin käyttötarkoitus ja käsittelyn oikeusperuste. Uusina asioina on rekisteröityä informoitava hänen oikeuksistaan ja tietojen säilytysajoista sekä tarjota tietosuojavastaavan yhteystiedot ja valitusohjeet. Rekisterinpitäjän tulee myös tiedottaa sekä rekisteröityjä että viranomaisia tietoturvaloukkauksista ja muista poikkeustilanteista [VAHTI-raportti 1/2016: 17]. Rekisteröidylle on tiedotettava:

- käsittelyn tarkoitus ja henkilötietoryhmät
- kenelle tietoja on luovutettu.
- tietojensäilytysaika ja sen perustelu
- rekisteröidyn oikeus tietojen oikaisuun sekä käsittelyn rajoittamiseen ja vastustamiseen
- mahdollinen tieto tietojen perusteella tehtävästä automatisoidusta päätöksenteosta tai profiloinnista
- käytetyt oikeussuojakeinot
- tietojen alkuperä, jos muu kuin rekisteröity itse.

Rekisteröity voi myös pyytää häneen liittyvän käsittelyn lopettamista, tietojen oikaisua tai poistoa. Hän voi myös vaatia, että automaattisen profiloinnin sijaan tietoja käsittelee ja päätöksen tekee ihminen. Nämä oikeudet eivät kuitenkaan ole absoluuttisia, vaan asetus määrittelee erilaisia perusteita, joihin tukeutuen rekisterinpitäjä voi pyynnöstä kieltäytyä.

Esimerkiksi erilaisten laillisten ja sopimuksellisten velvollisuuksien täyttäminen tai osapuolten oikeuksien suojaaminen.

2.6 Rekisterinpitäjän velvollisuudet

2.6.1 Oikeusperusta

Henkilötietojen käsittely on lainmukaista vain, jos sille on tietosuoja-asetuksessa määritelty peruste [Asetus 2016/679 2016: 36]. Näitä perusteita ovat:

- rekisteröidyn suostumus (esimerkiksi verkkopalvelut)
- rekisteröityä koskevan sopimuksen täyttäminen (esimerkiksi työsopimus)
- lakisääteinen velvoite (esimerkiksi työnantajavelvollisuudet)
- yleinen etu (kuten epidemioiden hoito)
- julkisen vallan käyttö
- luonnollisen henkilön elintärkeiden etujen suojaaminen (esimerkiksi terveydenhuolto).

Rekisteröidyn suostumuksesta asetus määrää tarkasti [Asetus 2016/679 2016: 37]. Rekisterinpitäjän pitää pystyä myöhemminkin osoittamaan, että suostumus on annettu ja että se on annettu vapaaehtoisesti. Esimerkiksi suostumuksen pyytämisen yhteydessä rekisteröityä on informoitava esimerkiksi rekisterinpitäjän henkilöllisyydestä ja tietojen käsittelyn tarkoituksesta.

Lakisääteinen tai julkisen vallan käyttöön liittyvissä perusteissa on jätetty kansallista liikkumavaraa. Oikeusministeriön julkaisemassa tietosuoja-asetuksen täytäntöönpanotyöryhmä on mietinnössään ehdottanut esimerkiksi, että kansallisesti sallitaan esimerkiksi julkisessa asemassa olevien henkilöiden asemaa koskevien tietojen käsittely [Nurmi ym. 2017: 50]. Samoin kansallisesti tullaan päättämään erityisiä henkilötietoryhmiä, kuten rikos- ja potilastietoja koskevasta käsittelystä.

Erityisen arkaluontoisen henkilötietoryhmien käsittely on lähtökohtaisesti kiellettyä [VAHTI-raportti 1/2016: 10]. Näitä ovat esimerkiksi tiedot rodusta tai etnisestä alkuperästä, poliittisista ja uskonnollisista vakaumuksista ja terveydestä. Oikeusministeriön työryhmä on kuitenkin esittänyt esimerkiksi, että vakuutuslaitoksilla olisi oikeus käsitellä näitä tällaisia tietoja vakuutusasioita hoitaessaan [Nurmi ym. 2017: 51]. Näiden ryhmien

käsittelyyn pitää olla peruste kuten rekisteröidyn suostumus, rekisterinpitäjän velvoitteiden täyttäminen tai henkilöiden etujen suojelu. Samoin yhdistykset ja muut vastaavat tahot saavat käsitellä jäsentensä ja muiden avainhenkilöiden tietoja mutta eivät luovuttaa niitä muille ilman kohteen suostumusta [Asetus 2016/679 2016: 38].

2.6.2 Oletusarvoinen tietosuoja

Asetus 2016/679 [2016: 48] käyttää termiä "sisäänrakennettu ja oletusarvoinen tietosuoja" (privacy by default). Rekisterinpitäjän tulee rajata käsiteltävät tiedot vain tarpeellisiin ja säilyttää niitä vain niin kauan kuin tarpeen. Myös henkilötietoihin käsiksi pääsy on rajattava tarpeellisiin henkilöihin, eivätkä tiedot saa lähtökohtaisesti olla julkisia.

Oletusarvoinen tietosuoja tarkoittaa myös, että rekisterinpitäjän on järjestettävä järkevät tekniset ja hallinnolliset toimenpiteet tietojen turvaamiseksi. Järkevyys määritellään ottamalla huomioon käytettävissä olevat keinot ja käsittelyn laajuus ja luonne sekä tietojen kohteen oikeuksille aiheutuva riski.

Käytännössä siis rekisterinpitäjien pitää arvioida käsittelyn riskit ja minimoida kerättyjen tietojen määrä, käsittelyn laajuus ja tietoihin pääsy. Teknisinä lisäkeinoina henkilötiedot voidaan esimerkiksi salata tai pseudonymisoida. Pseudonymisointi tarkoittaa henkilön tunnistetietojen korvaamista jollain välillisellä tunnisteella niin että henkilötietoja ei voida enää yhdistää henkilöön suoraan [VAHTI-raportti 1/2016: 11].

2.6.3 Tietoturvan hallinta

Monien tietosuoja-asetuksen velvoitteiden täyttäminen vaatii, että tietoturva on kiinteästi huomioitu organisaation toiminnassa. Tietojenkäsittelyn laajuudesta ja riskeistä riippuen se tarkoittaa esimerkiksi tietojenkäsittelyn vaikutusten arviointia, tietosuojavastaavan nimittämistä ja tietosuoja-asioiden jatkuvaa tarkkailua.

Vaikutustenarvioinnit ovat tietosuoja-asetuksen 35 artiklan pakottama käytäntö. Niistä käytetään esimerkiksi nimeä Data Protection Impact Analysis (DPIA) ja Privacy Impact Assessments (PIA). Ne ovat tärkeitä erityisesti, kun tietojenkäsittely sisältää kohdistuu arkaluontoisin tietoihin, jos käsittely on automaattista ja sillä on oikeusvaikutuksia tai jos valvotaan yleisölle avointa aluetta [Asetus 2016/679 2016: 53]. Vahti-raportti 1/2016

[2016: 21] kuitenkin suosittelee vaikutusarviointeja muillekin, sillä ne ovat hyvä keino varmistua tietojenkäsittelyn asetuksenmukaisuudesta.

Asetus 2016/679 määrittelee [2016: 54], mitä osia arviointiin on sisällyttävä. Näitä ovat erityisesi arviot käsittelytoimenpiteiden tarpeellisuudesta, riskeistä ja toimenpiteet riskien torjumiseksi. Jos käsittelyyn liittyvän riskin arvioidaan olevan korkea, eikä keinoja sen madaltamiseksi keksitä, tulee ottaa yhteyttä valvontaviranomaiseen, joka tarvittaessa ottaa kantaa tietojen käsittelyyn.

Maailmalla on jo useita hallinnollisia tietoturvastandardeja, jotka omaksuminen organisaation toiminnassa voivat olla hyvä lähtökohta tietosuoja-asioiden dokumentoituun harkintaan. Esimerkiksi ISO 27001 -standardi määrittelee joukon suositeltuja menettelytapoja, dokumentteja ja teknologioita tietosuojan hallinnointiin. ISO 27001 noudattaminen vaatii esimerkiksi tekemään määräajoin tietosuojaan liittyviä riskianalyysejä, joilla voidaan toteuttaa tietosuoja-asetuksen vaatimat vaikutustenarvioinnit [Freeman 2017].

Tietosuojavastaava (data protection officer) on pakko nimetä, jos tietojenkäsittelyä suorittaa julkishallinnon taho tai jos henkilötietojen käsittely on ydinosa rekisterinpitäjän liiketoimintaa, tai jos käsitellään erityisen arkoja henkilötietoryhmiä tai rikosasioita. Tietosuojavastaavan tehtävät on määritelty tarkkaan asetuksessa [Asetus 2016/679 2016: 56]: Hän neuvoo organisaatiota ja työntekijöitä tietosuoja-asetuksen noudattamisessa ja vaikutustenarviointien tekemisessä, seuraa asetuksen noudattamista ja tekee yhteistyötä valvontaviranomaisten kanssa. Hänen tulee myös olla rekisteröityjen saavutettavissa.

Organisaatio voi nimittää tietosuojavastaavaksi esimerkiksi työntekijän tai ulkoisen osapuolen. Merkittävää on, että tietosuojavastaava on mukana henkilötietojen käsittelyn suunnittelussa alusta asti ja ettei hänellä ole eturistiriitoja muiden tehtäviensä kanssa.

Asetuksen myötä monissa organisaatioissa tulee vahvempi tarve dokumentoidulle ja todistettavalle tietoturvalle. Vahti-raportti 1/2016 [2016: 20] suosittelee eri yksiköiden edustajista koostuvan tietosuojaorganisaation rakentamista ja tietosuojaan liittyvien tehtävien suunnittelua vuosikellomallilla. Vuosikello on työväline tietosuojan säännölliseen tarkasteluun ja kehittämiseen. Kuvassa 1 on esimerkki kvartaaleittain jaetusta tietosuojavuosikellosta. Se on tuttu monissa organisaatioissa esimerkiksi johdon strategiatyön kautta.

Vuosikellon avulla suunnitellaan toistuvat tehtävät kuten tietoturvadokumentaation, kehityshankkeiden ja tietoturvatapahtumien läpikäynti ja johdon raportointi. Myös koulutustarpeita on hyvä arvioida jatkuvasti.

Kuva 1. Yksinkertainen vuosikello tietosuoja-asioista. Mukailtu Vahti-raportista 1/2016 [2016: 21].

2.6.4 Tiedonanto ja yhteistyövelvoite

Asetuksessa on monia ehtoja, jotka tähtäävät tiedonkäsittely läpinäkyvyyteen. Tietosuoja-asetuksen 2016/679 33 ja 35 artikla [2016: 52] määrittävät pakolliseksi tietoturvaloukkauksista ilmoittamisen sekä valvontaviranomaiselle että rekisteröidylle 72 tunnin kuluessa loukkauksen havaitsemisesta. Ilmoituksen tulee sisältää mahdollisimman kattavat tiedot: Tapahtuman kuvaus ja altistuneiden rekisteröityjen määrät, tietosuojavastaavan tai muun yhteyshenkilön tiedot, arvioidut vaikutukset rekisteröidyille ja suunnitellut toimet vaikutusten lievittämiseksi.

Vahti-raportissa 1/2016 arvioidaan [2016: 26], että tämän velvoitteen täyttäminen vaatii kykyä havaita loukkaukset esimerkiksi automatisoituja lokitietoja analysoivia ohjelmistoja hyödyntämällä. Havainnoinnissa onnistuminen vaatii riittäviä resursseja ja mahdollisesti koulutusta. Raportti suosittelee, että organisaatiot suunnittelevat ja dokumentoivat sekä prosessit tietojärjestelmiensä tarkkailuun ja raportointiin, että valmistautuvat jo ennalta

kriisiviestintään esimerkiksi laatimalla ilmoitusvelvollisuuden täyttämistä helpottavia viestipohjia ja määrittelemällä kanavat joita pitkin sisäinen ja ulkoinen viestintä tehdään. Käsittelijöinä toimivat ja työasema- ja järjestelmäpalveluita tarjoavat IT-yritykset voivatkin olettaa, että sopimukset tulevat jatkossa sisältämään vaatimuksia tähän suuntaan.

Tietosuoja-asetuksen 2016/679 30 artikla [2016: 51] määrää, että rekisterinpitäjän on tehtävä seloste käsittelytoimista ja tarjottava se pyydettäessä valvontaviranomaiselle. Tämä voisi tapahtua esimerkiksi osana 5 artiklan [2016: 36] tietojen käsittelyn osoitusvelvollisuuden toteuttamisessa. Selosteessa tulee olla tiedot:

- käsittelyn tarkoituksista
- kerätyistä henkilötietoryhmistä
- tietojen luovutuksesta
- siirroista muihin maihin ja suojatoimista
- kuvaus teknisistä ja organisatorisista turvatoimista.

Seloste tulee olla, jos yrityksessä tai järjestössä on yli 250 työntekijää tai jos käsittely on toistuvaa, jos sen on todettu aiheuttavan korkean riskin tietojen kohteelle tai jos käsitellään erityisen arkoja henkilötietoryhmiä.

Rekisterinpitäjä on asetuksen 2016/679 31 artiklan mukaan [2016: 51] velvoitettu tekemään yhteistyötä valvontaviranomaisen kanssa. Yhteistyö voi alkaa viranomaisen pyynnöstä tai esimerkiksi vaikutustenarviointia tehtäessä havaitun korkean riskin aiheuttaman tarpeen johdosta. Yhteistyö kuuluu yleensä rekisterinpitäjän tietosuojavastaavan tehtäviin. Vahti-raportti 1/2016 myös suosittelee, että tietomurtotapauksissa tehdään yhteistyötä myös Viestintäviraston ja poliisin kanssa [2016: 30].

2.6.5 Tiedonsiirto Euroopan talousalueen ulkopuolelle

Asetuksen 2016/679 44 - 49 artikla [2016: 60] rajoittavat henkilötietojen siirtämistä Euroopan talousalueen (ETA) ulkopuolelle. Tietoja voidaan siirtää ilman erillistä lupaa maihin, joiden Euroopan komissio on katsonut pystyvän turvaamaan riittävän tietosuojan tason lainsäädännöllisesti ja hallinnollisesti. Tällä hetkellä komission on hyväksynyt vain noin tusina valtioita. Näistä huomattavimmat ovat Yhdysvallat, Kanada ja Sveitsi [Commission decisions on the adequacy of the protection of personal data in third countries 2017].

Tiedonsiirto Yhdysvaltoihin on sallittua vain, jos vastaanottava yritys on osallisena Privacy Shield -ohjelman puitteissa. Privacy Shield on Yhdysvaltojen kauppaministeriön valvoma ohjelma, johon liittyvät yritykset sitoutuvat noudattamaan sen asettamia sääntöjä ja ovat myös laillisesti vastuussa niiden noudattamisesta [Privacy Shield Program Overview 2017]. Kauppaministeriö ylläpitää myös listaa yrityksistä, jotka osallistuvat ohjelmaan. Näissä on jo mukana monia suuria toimijoita kuten Microsoft ja Google.

Tiedonsiirto muihin maihin on myös sallittua ilman erillistä lupaa, jos kumppanin toiminta on riittävän suojattua ja rekisteröidylle tarjotaan riittävä oikeussuoja [Asetus 2016/679 2016: 62]. Käytännössä tämä voi tarkoittaa esimerkiksi, että rekisterinpitäjän ja ulkomaisen toimijan välisissä sopimuksissa on mukana Euroopan komission hyväksymät tietosuojaa koskevat vakiolausekkeet. Asetuksen 2016/679 [2016: 63] 47 artikla mahdollistaa lisäksi monikansallisen yrityksen sisäiset siirrot ilman eri lupaa, jos yritys on laatinut tietyt vaatimukset täyttäviä sen kaikkia yksiköitä sitovat säännöt.

Omien toimiensa lisäksi organisaation on hyvä kartoittaa myös käyttämänsä palvelut ja muut järjestelmät, joiden sisällä tieto saattaa liikkua EU-alueen rajojen ulkopuolelle. Pilvipalveluita henkilötietojen käsittelyyn käyttävien organisaatioiden on hyvä tarkistaa voiko palvelussa määrätä tietojen maantieteellisen sijainnin. Myös esimerkiksi pilvessä toteutettu sähköposti- tai verkkolevypalvelu voi huonolla tuurilla tallentaa dataa ulkomaille.

2.7 Käsittelijän velvollisuudet

Henkilötietojen käsittelyä tekeville tahoille on määrätty vaatimuksia tietosuoja-asetuksen 2016/679 28 artiklassa [2016: 49]. Perusvaatimus on, että käsittelijän on toteutettava asetuksen vaatimukset täyttävät tietosuojatoimenpiteet. Käsittelijä toimii aina rekisterinpitäjän kanssa tehdyn sopimuksen nojalla eikä käsittelijä saa vuorostaan ulkoistaa käsittelyä kolmannelle osapuolelle ilman rekisterinpitäjän lupaa. Käsittelijän pitää noudattaa rekisterinpitäjän antamia kirjallisia ohjeita, paitsi jos ne ovat lainvastaisia. Laki saattaa myös vaatia käsittelijää tekemään sellaisiakin toimenpiteitä joita rekisterinpitäjä ei ole määrännyt.

Suurin osa käsittelijä vaatimuksista tuleekin rekisterinpitäjän ja käsittelijän välisten sopimusten myötä. Käsittelyyn osallistuvan henkilöstön pitää sitoutua salassapitovelvollisuu-

den noudattamiseen. Rekisterinpitäjän tarvitsee muiden käsittelytoimien lisäksi tehdä yhteistyötä rekisteripitäjän kanssa esimerkiksi rekisteröityjen oikeuksien turvaamiseksi ja tietoturvaloukkausten jälkipyykin selvittämiseksi. Vahti-raportissa 1/2016 [2016: 28] suositellaan myös, että sopimuksissa huomioidaan palvelun laadun seuranta ja raportointi.

Asetuksen 2016/679 30 artiklan [2016: 51] mukaan käsittelijöiden tulee ylläpitää selosteita käsittelytoimistaan. Selosteen tulee sisältää kutakuinkin samat tiedot kuin rekisterinpitäjien vastaavassa selosteessa.

2.8 Vastuunjako ja sopimukset

Rekisterinpitäjän, käsittelijän ja muiden alihankkijoiden vastuut määräytyvät pitkälle sopimuksin. Tietosuoja-asetus määrittelee osittain sopimusten pakollisen sisällön ja niiden vaikutukset. Terho Nevasalon ja Sami Tenhusen mukaan [2017: 26] vastuunjako käsittelyn alihankintaketjun osapuolten mukaan jakaantuu seuraavasti:

Rekisterinpitäjällä on valtuudet myöntää käsittelyoikeudet käsittelijälle ja vastaa ohjeidensa lainmukaisuudesta. Rekisterinpitäjän tulee huolehtia, että käsittelijä kykenee huolehtimaan tietosuoja-asetuksen velvoitteiden täyttämisestä.

Käsittelijällä on velvollisuus noudattaa rekisterinpitäjän ohjeita ja varmistua niiden lainmukaisuudesta. Käsittelijä vastaa mahdollisen alihankkijansa menettelystä rekisterinpitäjään.

Alihankkijan asema ja korvaus- ja avustamisvastuu määräytyvät sopimuksellisesti. Jotta alihankkijaa voidaan käyttää, on se sisällyttävä jo rekisterinpitäjän ja käsittelijän väliseen sopimukseen.

Asetuksen 2016/679 81 artiklan mukaan [2016: 81] henkilölle aiheutuneesta vahingosta voidaan asettaa vastuuseen yhtä hyvin rekisterinpitäjä kuin käsittelijäkin. Käsittelijä on kuitenkin vastuussa vain, jos se on toiminut joko asetuksen määräyksiä tai rekisterinpitäjän laillista ohjeistusta huomioimatta. Nevasalo ja Tenhunen kuitenkin tähdentävät [2017: 27] että rekisterinpitäjä ja käsittelijä voivat sopia korvausvelvollisuudesta esimerkiksi siten, että rekisterinpitäjä vastaa taloudellisista seuraamuksista, jos rekisterinpitäjän ohjeistama käsittely myöhemmin osoittautuu lainvastaiseksi.

Rahallinen vastuu virhetilanteissa ja asetusten vastaisessa toiminnassa voi käsittää sekä rekisteröidylle koituneen haitan korvauksia että hallinnollisen sakon. Asetuksen 2016/679 83 artiklan [2016: 82] nojalla ensimmäisestä virheestä määrättävä hallinnollinen sakko on suurimmillaan 10 miljoonaa euroa tai 2 % yrityksen liikevaihdosta, kumpi vain on korkeampi.

3 Valmistautuminen ohjelmistopalveluyrityksessä

3.1 Nykytila-analyysi

Yrityksen GDPR-valmiuden tutkiminen aloitetiin nykytila-analyysilla. Analyysin runkona käytetiin Vahti-raportin 1/2016 kuvailemaa menettelyä [2016: 31]. Työ aloitettiin henkilötieto- ja sopimusinventaarion teolla. Sen tarkoituksena oli muodostaa kattava kuva niistä henkilörekistereistä, joiden rekisterinpitäjä yritys on, sekä asiakassopimuksista ja niiden myötä tehtävästä henkilöstörekisterien käsittelystä. Suurin osa tiedoista kerättiin yrityksen henkilökuntaa haastattelemalla.

Nykytila-analyysin tukena käytettiin Valtiovarainministeriön Vahti-työryhmän tekemää Tietosuojan tukityökalua. Tukityökalu on Vahti-raportin 1/2016 tueksi tehty vapaasti saatavilla oleva Excel-taulukko, jonka voi ladata https://www.vahtiohje.fi -sivustolta. Se auttoi hahmottamaan tietosuoja-asetuksen osiot ja niiden vaatimukset omassa organisaatiossa ja valmistelutyön valmiusasteen. Tietosuojatyökalun päänäkymä on esitetty kuvassa 2.

	A	B	C	E
1	**Tietosuojan tukityökalu - TIKU**			
2	ver 1.00 - 4.10.2016			
4	**VAHTI raportti 1/2016 osa-alue**			
5		**Tehtävä | toimenpide | raportissa kuvattu osa-alue, joka organisaation on käytävä läpi [riittävä ymmärrys | osaaminen]**	**Nykytilan arviointi**	**Tavoitetila**
6	**4. Rekisteröidyn oikeudet**	**Keskiarvo osa-alueesta:**	**1,21**	
7		4.1 Rekisterinpitäjän tiedonantovelvoitteet	50% valmiina	Huolehditaan ohjeistuksella ja koulutuksella
8		4.2 Oikeus saada pääsy tietoihin	50% valmiina	Jokin muu ratkaisu
9		4.3 Oikeus tietojen oikaisemiseen	Ymmärretty	Jokin muu ratkaisu
10		4.4 Oikeus poistaa tiedot (”oikeus tulla unohdetuksi”)	50% valmiina	Jokin muu ratkaisu
11		4.5 Oikeus siirtää tiedot järjestelmästä toiseen	50% valmiina	Jokin muu ratkaisu
12		4.6 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia	Ymmärretty	Huolehditaan ohjeistuksella
13		4.7 Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta	100% valmiina	Vaatimustenmukainen
14	**5 Rekisterinpitäjän velvollisuudet**	**Keskiarvo osa-alueesta:**	**-0,40**	
15		5.1 Käsittelyn oikeusperusta	Hyväksytty | Ei koske meitä	Huolehdittava sopimuksella | hallintopäätöksellä
16		5.2 Tietosuojan hallinnointi, roolit ja vastuut	*** valitse listalta ***	Huolehdittava sopimuksella | hallintopäätöksellä
17		5.2.1 Tietosuojavastaava		
18		Tietosuojavastaavan nimeäminen ja oikea asema organisaatiossa	100% valmiina	Huolehdittava sopimuksella | hallintopäätöksellä
19		Tietosuojavastaavan tehtävänkuva	100% valmiina	Huolehdittava sopimuksella | hallintopäätöksellä
20		5.2.2 Tietosuojaorganisaatio	Työ aloitettu	Huolehditaan ohjeistuksella ja koulutuksella
21		5.2.3 Vuosikello	Työ aloitettu	Huolehditaan ohjeistuksella ja koulutuksella
22		5.3 Tietosuojariskienhallinta	50% valmiina	Huolehditaan ohjeistuksella ja koulutuksella
23		5.3.1 Tietosuojan vaikutustenarvioinnit	100% valmiina	Vaatimustenmukainen

Kuva 2. Tietosuojan tukityökalu

Huomattiin nopeasti, että yrityksen omat henkilörekisterit ovat vähäpätöisiä asiakkaille tehtävään henkilötietojen käsittelytyöhön verrattuna. Kuitenkin tietosuoja-asetuksen mukaan yrityksen tulee varmistaa, että sen rekisteriselosteet ovat asetuksen tasalla ja sen omat rekisterit on huomioitu tietoturvadokumentaatioissa. Yritys on rekisterinpitäjä esimerkiksi omille työntekijöiden ja asiakkaiden yhteyshenkilöiden tietoja sisältäville rekistereille.

Kaikissa asiakassopimuksissa ei ollut kirjaimellisesti tulkittavissa olevia ohjeita henkilötietojen käsittelyyn tai tietoturvan seurantaan. Samoin tietojen elinkaarta ei aina ole määritelty. Jotkut asiakkaista olivat kuitenkin jo itse aktivoituneet GDPR-säädöksen tuomien muutosten hallinnointiin ja alkaneet pyytää tarkempaa selontekoa yrityksen tietoturva-asioista.

Inventaarion jälkeen arvioitiin henkilötietojen käsittelyn riskejä sekä teknisestä että hallinnallisesta näkökulmasta. Yrityksen pienen koon vuoksi tietoturvavastuut ja suunnittelu ovat yrityksessä aina olleet yrityksen omistajien käsissä, ja he ovat myös olleet avainhenkilöitä kaikessa yrityksen tekemässä tuote- ja järjestelmäsuunnittelussa. Yrityksen tuotteissa ja toiminnassa on sen seurauksena ollut toimiva mutta vähäisesti dokumentoitu lähestymistapa tietosuoja-asioihin.

Suurin osa yrityksen tietoturvadokumentaatiosta oli luotu sisäistä käyttöä varten. Todettiin, että EU:n tietosuoja-asetuksen myötä olisi aiheellista varautua tietosuoja-asioiden osoittamiseen. Sekä asiakkaat että viranomaiset voivat vaatia dokumentoidumpia ja hallinnoidumpia tietosuojakäytäntöjä.

Päätettiin myös aloittaa selvitys yrityksen virallisen tietosuojavastaavan nimittämiseksi. Tämä katsottiin tarpeelliseksi siksi, että henkilötietojen käsittely on yrityksen ydintehtäviä. Asetuksen kannalta yrityksen koolla ei ole merkitystä tietosuojavastaavan nimitysvaatimukselle.

Yrityksen tietojärjestelmät jaettiin karkeasti kahteen osaan: työntekijöiden käyttämiin ja asiakkaille myytyjen palveluiden ylläpitoon. Yrityksessä oli jo meneillään 2016 käynnistynyt sisäisten järjestelmien, työasemien ja palvelinympäristön tietoturvan kehitysprojekti. Projektin aikana oli kartoitettu kehityskohteita ja niistä useita oli jo parannettu. Jäljellä olevista kehityskohteista muutama nostettiin nyt tietosuoja-asetuksen valossa kiireelliseksi.

Yrityksen verkko- ja palvelinlaitteet todettiin suurimmilta osin asianmukaisiksi. Päätettiin vaihtaa yrityksen käyttämät palomuurilaitteet uudemman sukupolven IPS/IDS (Intrusion Prevention system / Intrusion Detection System) -teknologioilla varustettuihin malleihin ja tarkistuttaa, että palomuurilaitteistot ovat asianmukaisesti konfiguroitu. Näillä toimenpiteillä haluttiin tietoturvan parantamisen lisäksi varmistaa, että yritys kykenee tarjoamaan parempaa seurantatietoa palvelimien tietoliikenteestä ja myös aktiivisesti havaitsemaan mahdolliset hyökkäykset.

Palvelinlaitteita ja konesalikäytäntöjä tutkittaessa todettiin, että palvelinten tilaa seurattiin hyvin ja tietoturvapäivityksistä huolehdittiin aktiivisesti, mutta näihin toimenpiteisiin liittyvä dokumentaatio ei aina ollut saatavilla. Verkkoinfrastruktuurin ja palvelinylläpidon dokumentointi suunniteltiin ja aloitettiin erillisenä projektina.

Yrityksen fyysiset puitteet katsottiin turvallisiksi. Analyysissä arvioitiin yrityksen toimistotilat ja palvelinsali. Riskejä tutkittiin monelta eri näkökannalta: Luonnonilmiöiden, infrastruktuurin kuten sähkönjakelun ja rikosten suhteen. Toimipisteiden ulkopuolella tapahtuvaan työskentelyyn kuten asiakkaiden toimipisteissä ja muualla tehtävään etätyöhön liittyviä riskejä oli pyritty kontrolloimaan esimerkiksi työasemien tallennusmedioiden kattavalla salauksella ja suojatuilla Virtual Private Network (VPN) -yhteyksillä.

Nykytila-analyysissa arvioitiin myös henkilökunnalle suunnatun tietoturvaohjeistuksen ja -koulutuksen tasoa. Selvityksen perusteella todettiin, että ohjeita tulisi päivittää ja lisätä etenkin ohjelmistokehittäjille tarjottavan koulutuksen määrää. Samoin uusien työntekijöiden perehdytysmateriaalia ja työntekijöiden työsopimusten päätymisiin liittyviä käytäntöjä parantaa. Yritys ei myöskään ollut huomannut hyödyntää vertaisoppimisen keinoja johdonmukaisesti. Paljon olemassa olevaa tietoturvatietämystä oli jäänyt piiloon muutaman asiantuntijan taakse.

Yrityksen ohjelmistotuotteiden tietoturvan tilaa oli jo aiemmin tutkittu määräajoin, usein uusien tai vanhojen asiakkaiden tietoturvaprojektien yhteydessä tilatuissa asiantuntijayritykseltä tilatuissa tietoturvakartoituksissa ja haavoittuvuustestauksissa. Näissä testauksissa ilmenneet tietoturva-aukot oli välittömästi korjattu. Todettiin, että yrityksen sisäistä testausta kannattaisi vielä kehittää. Yhdessä koulutustarpeiden huomioinnin kanssa tuotteen tietoturvataso voitaisiin nostaa entistä paremmalle tasolle kohtalaisin kustannuksin.

Myös yrityksen tiedotusvelvollisuuden toteutuminen arvioitiin. Rekisteri ja käsittelytoimien selosteet eivät olleet vielä tietosuoja-asetuksen vaatimalla tasolla. Samoin kriisiviestintää ei ole valmisteltu niin kattavasti kuin esimerkiksi Vahti-raportissa 1/2016 on suositeltu [2016: 34].

Nykytila-analyysin perusteella valittiin kaksi kehityskohdetta tämän opinnäytetyön puitteissa tehtäväksi: Yrityksen tietoturvadokumentaatioon selkiyttäminen ja ohjelmistotuotteen toiminnalliset vaatimukset tietosuoja-asetusten määrittämien rekisteröidyn oikeuksien täyttämisen automatisoinniksi. Muita priorisoituja kehityskohteita olivat henkilötietojen elinkaaren haltuunotto ja yrityksen sisäinen käyttäjänhallinta.

3.2 Tietoturvan dokumentointi

Dokumentointi aloitettiin kokoamalla yhteen ja päivittämään aikaisemmin hajanaisemmin kirjattu yrityksen tietoturvasuunnitelma. Dokumentointiin osallistuivat myös yrityksen toimitusjohtaja sekä pääarkkitehti. Muulta henkilöstöltä kerättiin haastatteluin tietoa heidän osaamisalueidensa järjestelyistä.

Tietoturvasuunnitelmaan sisällytettiin nykytiedot yrityksen fyysisestä ja tietoteknisestä turvallisuudesta sekä henkilöstöturvallisuudesta. Tämä tehtiin laatien yritykselle vapaamuotoinen tietotilinpäätös. Sen tavoitteena oli kuvata tietojenkäsittelyn kokonaiskuva erityisesti yrityksen johtoa varten. Tietotilinpäätöstä alustettiin miettimällä keskeisiä kysymyksiä, joiden vastausten tulisi olla kirjallisia ja helpommin löydettävissä. Näitä olivat:

- Mitä tietoja yritys kerää, kuka niihin pääsee käsiksi ja miten?
- Tunnistetaanko, milloin henkilötietoja muodostuu?
- Voidaanko osoittaa kerättyjen tietojen tarpeellisuus?
- Tiedetäänkö mitä on kiellettyä kerätä ja mitkä tiedot ovat arkaluontoisia?
- Onko tietojen käsittelytavat kuvattu ja käsittelyselosteet kunnossa?
- Käsittelyä tietoja organisaation ulkopuolella?
- Ovatko asiakas ja alihankinta sopimukset tietosuoja-asetuksen mukaisia?
- Tietävätkö työntekijät mitä käsittelytoimia saa tehdä?
- Ovatko keskeiset vastuut ja tehtävät määritelty johdon taholta?
- Ovatko rekisteröityjen oikeudet tiedossa ja miten ne mahdollistetaan?
- Noudatetaanko yleisiä tietoturvaperiaatteita? Onko ne tiedotettu intrassa tai muualla?

- Tiedetäänkö milloin yrityksellä ilmoitusvelvollisuus viranomaisille tai asiakkaille?
- Onko nimetty tietosuojavastaava?
- Pystytäänkö todentamaan suostumus tietojen keruuseen?
- Miten tietosuoja ja -turva suojaan koulutusta ja tiedostusta hallinnoidaan?

Tietoturvasuunnitelman teknisenä näkökulmana keskityttiin yrityksen ylläpitämien asiakassovellusten, palvelinsalin ja laitteiden turvallisuuden ja saatavuuden turvaamiseen. Tutkittiin myös, ovatko yrityksen tekniset ylläpito- ja seurantatoimenpiteet mitoitettu riskien mukaisesti ja hoidettu aktiivisesti. Myös ohjelmistokehitykseen liittyviä asioita pohdittiin erityisesti henkilöstön koulutuksen ja jatkuvan ja dokumentoidun tietoturvatestauksen varmistamisen puitteissa.

Tietoturvasuunnitelman rinnalla aloitettiin yrityksen asiakkailleen ylläpitämien www-palveluiden kartoitus ja niihin liittyvien tietoturvaratkaisujen inventointi. Suurelle osalle yrityksen asiakkaista oli tehty räätälöityjä palveluratkaisuja, jotka vaativat erilaisin tekniikoin toteutettuja järjestelmiä. Myös asiakaskohtaiset käsittelysäännöt ja esimerkiksi moninaisin eri tavoin muodostettavat suojatut tietoliikenneyhteydet yrityksen ja asiakkaiden tietojärjestelmien välillä olivat osoittautuneet toisinaan haastaviksi erityisesti yrityksen asiakastukitiimille, jotka työskentelevät päivittäin monien erilaisten tapauksien ja asiakkaiden parissa. Tarkemmilla ohjeilla ja käytäntödokumenteilla toivotaan olevan tehostava vaikutus työskentelyyn näiden monitahoisten ympäristöjen kanssa.

Tietoturvasuunnitelman perusteella laadittiin asiakkaille suunnattu esite yrityksen tietoturvaratkaisuista yleisesti ja tietosuoja-asetuksen voimaantulon huomioinnista erityisesti. Esitettä on tarkoitus käyttää jatkossa sopimusneuvottelujen pohjatyössä, jotta tietosuoja olisi entistä paremmin esillä uusia asiakasympäristöjä suunnitellessa.

Yrityksen sisäiset tietoturvaohjeet ja käyttösäännöt päivitettiin. Ohjeet suunniteltiin koko henkilöstön yleisohjeiksi. Niihin kerättiin paitsi tietoteknisiä ja fyysisiä ohjeita, myös yleisiä sosiaalisen tietoturvan piiriin kuuluvia asioita, jotta haavoittuvuus erilaisille huijauksille ja muulle sosiaalisille tietoturvauhkille vähenisi. Ohjeistuksella pyrittiin myös siihen, että työntekijät varmasti käyttäisivät tietoturvallisia yhteyksiä päivittäisessä toiminnassaan ja huolehtisivat laitteidensa salauksesta. Myös henkilötietojen käsittelyyn liittyviin asioihin kuten niiden siirtämiseen ja säilöntään tehtiin yhteiset säännöt. Lisäksi päätettiin alkaa keräämään kuittaukset ohjeiden lukemisesta.

Suurin osa yrityksen henkilöstöstä tekee ohjelmistokehitystä. Ohjelmistokehittäjien koulutusta päätettiin kehittää. Merkittävänä osana tulee olemaan kaksi kertaa kuukaudessa järjestettävät sisäiset koulutustuokiot, joissa käydään läpi sekä yleisiä periaatteita että tietoturvauutisia, jotka vaikuttavat kehittäjien työhön. Yrityksessä alettiin myös valmistelemaan työntekijöiden sertifioinnin tukemista.

Turvasuunnitelman liitteeksi alettiin valmistelemaan kriisiviestintäohjeita ja pohjia. Näitä ovat esimerkiksi tietoturvaviranomaisille ja rekisteröidyille tahallisen tai tahattoman tietoturvaloukkauksen tapahtuessa lähetettävät ilmoitukset. Etukäteissuunnitelmia valmisteltiin myös esimerkiksi tietojen saatavuuden vaarantamien tapausten varalle. Samalla havaittiin, että henkilökunnalle voisi järjestää myös harjoittelua erilaisten ongelmatilanteiden varalle. Kriisitilanteessa on muutoin vaikeampi toimia rauhallisesti ja määrätietoisesti.

3.3 Jatkotoimenpiteet

Nykytila-analyysin ja tietoturvasuunnitelman avulla tunnistettiin useita kehityskohteita. Ne jaettiin hallinnollisiin ja teknisiin muutoksiin. Tekniset muutokset jaettiin edelleen infrastruktuurin kehitykseen ja yrityksen ohjelmistotuotteiden ja räätälöityjen sovellusten kehitykseen.

Eri työkohteita löydettiin paljon ja niitä tullaan työstämään jatkuvasti. Tämän opinnäytetyön puitteissa tehtäväksi valittiin erityisesti ohjelmistotuotteeseen toteutettavat rekisteröidyn oikeuksien automatisoidun ja taloudellisen järjestämisen mahdollistavat ominaisuudet sekä tietojen käsittelyn seurattavuuteen liittyvät parannukset. Pidettiin merkittävänä, että asiakkaille voidaan tarjota mahdollisimman valmis paketti, jolla he voivat tuotetta käyttäessään täyttää asetuksen tekniset ja käytännölliset vaatimukset. On havaittu, että useilla asiakkailla ei vaikuta vielä olevan kovin selkeää kuvaa, mitä vaatimuksia tietosuoja-asetus tulee heille rekisterinpitäjänä asettamaan tai mielipiteitäkään siitä, miten niitä ohjelmistoissa huomioitaisiin.

4 Ohjelmistotuotteen muutokset

4.1 Tuotteen yleiskuvaus

Työn tilanneen yrityksen merkittävin ohjelmistotuote on henkilötietoja käsittelevä web-palvelu. Sitä on ja kehitetty ja laajennettu jo yli kymmenen vuoden ajan. Se on toteutettu DotNetNuke (DNN) -sisällönhallinta-alustan päällä toimivana ASP.NET -sovelluksena, joka käyttää tietovarastonaan relaatiotietokantaa. Tuotteesta on muutama kymmenen asiakaskohtaista asennusta eri WWW-palvelimilla. Yritys ylläpitää näistä useimpia ja loput ovat asiakkaiden omia palvelimia. Tuotteella on satoja pää- ja ylläpitokäyttäjiä ja satoja tuhansia loppukäyttäjiä. Tuotetta käytetään sekä asiakkaiden sisäisiin toimintoihin että asiakkaiden julkisten verkkopalveluiden tietojärjestelmänä.

Arkkitehtuurisesti ohjelmisto on jaettu useisiin mahdollisimman itsenäisiin moduuleihin: Kukin moduuli sisältää tarvittavat kerroksittain jaetut toiminnot käyttöliittymästä tietokantatoimintoihin. Tuote on alun perin tehty ASP.NET Web Forms -tekniikalla mutta erityisesti loppukäyttäjille suunnattuja osia on alettu pikkuhiljaa modernisoimaan eriyttäen käyttöliittymä ja toimintalogiikka esimerkiksi React-JavaScript -kirjastolla toteutettuun osaan ja Representational State Transfer (REST) -rajapintoihin.

Tuotteen erityispiirteenä on asiakaskohtainen räätälöinti. Kukin asiakas voi itse päättää, mitä tuotteen ominaisuuksia se käyttää ja miten ne toimivat. Esimerkiksi tapahtumaan ilmoittautumiseen voidaan liittää hakemustoiminto, jonotusjärjestelmä tai muita toimintoja ja voidaan määritellä mitä henkilötietoja järjestelmä käsittelee. Myös tuotteen ulkoasun räätälöidään usein kunkin asiakkaan toivomusten mukaisesti. Lisäksi tuotetta on pikkuhiljaa laajennettu sen päätarkoitusta tukeviin toimintoihin, kuten virkavapaahakemuksiin ja organisaatioiden kehityskeskusteluihin. Valitettavasti tämä muokattavuus aiheuttaa omat haasteensa tuotteen ohjelmistokehitykselle ja asettaa paljon paineita tuotteen testaukselle ja eri konfiguraatioiden huomioinnille.

Tuotetta tukee useita kymmeniä erillisiä rajapintasovelluksia. Näistä suuri osa on ohjelmoitu siirtämään henkilötietoja ja muuta dataa yrityksen ja sen asiakkaiden tietojärjestelmien välillä. Näiden tekninen toteutus, samoin kuin tiedonsiirtojen turvaamisen käytännöt, vaihtelevat laidasta laitaan asiakkaiden tarpeiden mukaisesti.

4.2 Asiakkaiden erojen huomiointi

Vaikka ohjelmisto pyrkii tuotteenomaisuuteen, asiakaskohtaisten räätälöintien myötä on syntynyt ikäviä epäyhtenevyyksiä sekä käyttöliittymässä, toiminnassa ja tietokantatasolla. Useilla asiakkailla on omia erityisvaatimuksia sen suhteen, miten tuotteen tulee hoitaa esimerkiksi tapahtumiin ilmoittautuminen ja jonotus, laskutus tai vaikka kehityskeskustelujen pitoon liittyvät prosessit. Laadultaan merkittäviä ja laajoja räätälöintejä järjestelmässä on useita kymmeniä ja pienempi sadoittain.

Räätälöinnit aiheuttavat ongelmia ohjelmistokehityksessä erityisesti siksi, että tuotteen dokumentaatio ei aina ole pysynyt ajan tasalla kaikkien asiakkaiden osalta. Aina ei ole selkeää, miten tuotteen kuuluu toimia tietyssä tapauksessa.

Asiakaskohtaisten tietokantojen perusrakenne on yhtenevä, mutta toisinaan eroaa muutamien sarakkeiden tai asiakaskohtaisten tietokantataulujen osalta toisistaan. Tietoja on myös tallennettu osittain siten, että pelkästään taulujen ja sarakkeiden nimien perusteella ei voi päätellä, missä kaikkialla henkilötietoja saattaa sisältää. Asiakkaat ovat voineet myös itse lisätä henkilötietokenttiä järjestelmän joihinkin toimintoihin kuten tapahtumailmoittautumisten yhteydessä kysyttäviksi lisätiedoiksi.

Tietosuoja-asetuksen vaatimuksia toteuttaessa asiakaskohtaiset erot päätettiin pyrkiä huomioimaan asiakas kerrallaan. Päätettiin tehdä selkeä perustoiminnallisuus, jota sitten laajennetaan asiakkaiden toivomusten mukaan. Rekisterinpitäjät itse määrittelevät esimerkiksi henkilötietojen käsittelyn oikeusperustan ja käsittelytavat. Joissakin tapauksissa reksiterinpitäjillä saattaa esimerkiksi olla laillinen velvoite säilyttää tiettyä dataa kuten laskutustietoja pitempään kuin toisilla ja sen perusteella tarve kieltäytyä poistamasta niitä rekisteröidyn pyynnöstä huolimatta.

Tuotteen ominaisuuksien on tarkoitus tukea rekisteröityjen oikeuksien taloudellisesti kannattavaa toteutumista: Rekisteröity voitaisiin esimerkiksi unohtaa eli poistaa tietokannasta käsinkin, mutta suurien käyttäjämäärien kanssa siitä tulisi nopeasti suuri kuluerä rekisterinpitäjille.

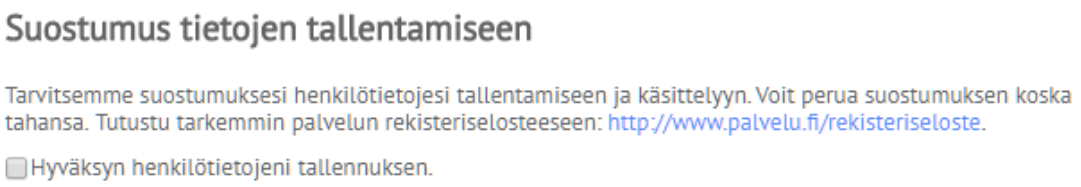
Käytännössä asiakkaiden kanssa tullaan käymään yksi kerrallaan sopimusneuvottelut, joissa huomioidaan tarkemmin tietosuoja-asetuksen mukaiset ehdot esimerkiksi käsittelyjen ohjeistuksesta ja GDPR-toimintojen käyttöönotosta. Samalla tehdään projektityönä

tarvittavat muutokset ja laajennukset tietosuojatoimintoihin ja järjestetään asiakaskohtainen hyväksymistestaus. Useiden asiakkaiden kanssa tarvitsee myös sopia, miten tieto esimerkiksi unohtamispyynnöstä viedään asiakkaan muihin tuotteeseen kytkettyihin järjestelmiin.

4.3 Suostumuksen pyyntö

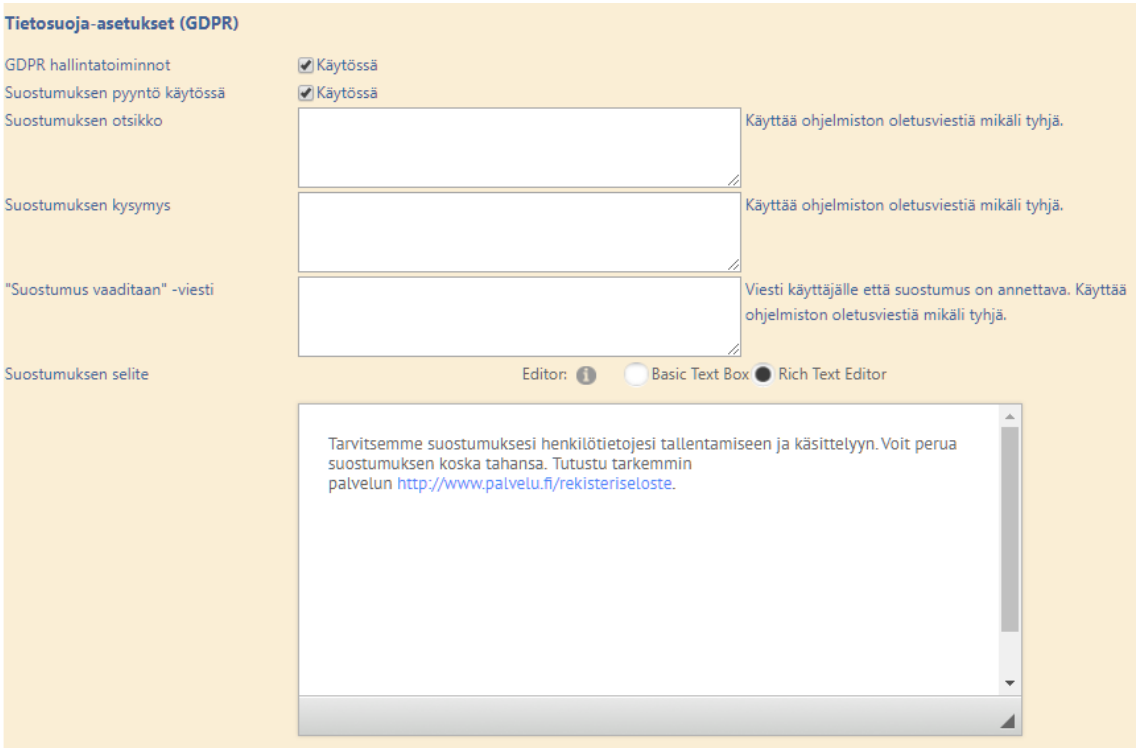
Ohjelmistotuotteeseen tehtiin uusi toiminto rekisteröidyn suostumuksen pyytämiseksi. Tuotetta kuluttajien palvelemiseen käyttävät vahvistavat sen avulla, että heillä on laillinen peruste näiden käyttäjien henkilötietojen käsittelemiseen. Tuotteen pitkän historian aikana siihen on muodostunut useita kymmeniä sisääntulokohtia, joissa uusilta käyttäjiltä kerätään henkilötietoja. Näitä ovat paitsi ilmoittautumismoduuli, myös erinäiset yhteydenottopyyntö- ja palautuslomakkeet ja käyttäjätilin rekisteröintimoduuli. Käytännössä suostumus on pyydettävä sillä hetkellä, kun ensimmäisiäkään henkilötietoja järjestelmään aiotaan tallentaa, jos rekisterinpitäjällä ei ole muuta käsittelyperustetta.

Ominaisuuden toteutustapaa suunniteltaessa todettiin, että tuotteen ydinmoduulien välillä on jo muutenkin riippuvuuksia ja käytännössä kaikille asiakkaille on asennettu tietty joukko moduuleita riippumatta heidän erityistarpeistaan. Ylläpidettävyyden parantamiseksi ja kahdennetun koodin välttämiseksi päätettiin luoda yhteinen ASP.NET -kontrolli, jota eri moduulit voivat hyödyntää. Kontrolliin sisällytettiin tapa valita toimintamoodi siten, että sitä voidaan hyödyntää sekä perus- että ylläpitokäyttäjien toiminnoissa. Kuvassa 3 on esimerkki loppukäyttäjälle näytettävästä suostumuksen pyynnöstä.



Kuva 3. Suostumuksen pyyntö -ominaisuuden käyttöliittymä loppukäyttäjälle.

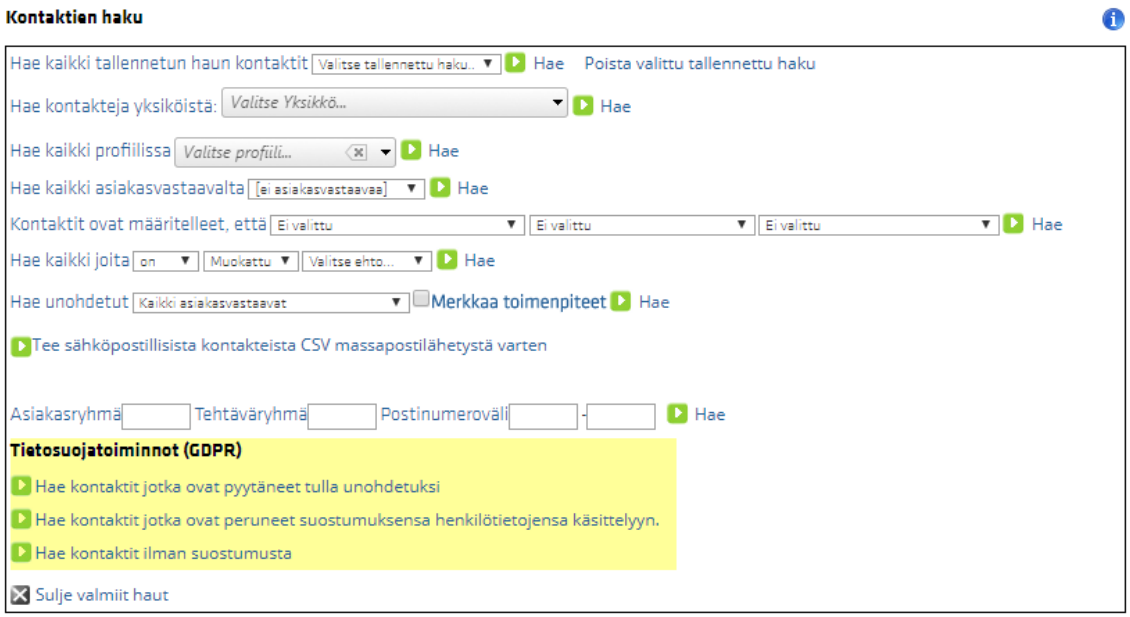
Tietosuoja-asetus edellyttää, että käyttäjää informoidaan henkilötietojen käsittelystä ja hänen oikeuksistaan suostumuksen antohetkellä. Tätä varten kontrollin kaikki tekstisisällöt tehtiin luettavaksi tuotteen asetuksista, jotka on esitetty kuvassa 4. Näin kunkin asiakkaan ylläpitäjät voivat syöttää tarvittavat rekisteriselosteet ja muut tiedot kontrollissa näytettäväksi.



Kuva 4. Tietosuojatoimintojen asetusten hallintakäyttöliittymä

Koska suostumuksen saanti on pystyttävä osoittamaan, ohjelmoitiin sen tallennus kirjoittamaan tavanomaista tarkemmat lokitiedot tapahtumasta. Myös suostumuksen peruutus kirjataan tarkoin.

Tuotteessa oli jo valmiina ’Valmiit haut’ toiminto henkilöiden etsimiseen, joka on esitetty kuvassa 5. Sen osaksi lisättiin mahdollisuus hakea suostumuksensa peruuttaneet henkilöt. Asiakkaat itse päättävät miten jatkavat näiden henkilöiden käsittelyä järjestelmässä.



Kuva 5. Henkilöiden valmiit haut -toiminto.

Monien asiakkaiden ympäristöissä on mahdollista, että yksi käyttäjä voi luoda järjestelmään esimerkiksi tunnistautumattoman ilmoittautumisen kautta useita henkilötietueita itselleen. Tuotteessa on jo mahdollisuus yhdistää näitä tietueita toisiinsa tuplien poistamiseksi, mutta todennäköisesti suostumuksen pyytämistä ja unohdus-toimintoa varten tutkitaan, miten tämä tuplien käsittely voitaisiin automatisoida. Tavoitetila olisi, että yhden käyttäjän henkilötietoihin kohdistuvat toimet ovat yksiselitteisiä eikä niin että toisessa tietueessa suostumus on merkitty annetuksi ja toisessa ei.

4.4 Tietojen siirto

Rekisteröidyn oikeuksiin kuuluu myös mahdollisuus pyytää omat tietonsa jossain yleisesti käytössä olevassa koneluettavassa muodossa. Siirron kannalta oleellista dataa tuotteessa katsottiin olevan rekisteröidyn henkilötiedot ja esimerkiksi hänen osallistumistietonsa eri tapahtumiin ja profiilitiedot kuten osaamisprofiilit. Kaikki data koostuu yksinkertaisista perustietotyypeistä kuten merkkijonoista, numeroista ja päivämääristä. Toteutuksessa päätettiin rajata tietojen haku tuotteen kontaktitietoihin, mutta se on helposti laajennettavissa myös mahdollisiin DNN-alustan käyttäjätunnustietoihin, mikäli tarpeen. Ainakaan vielä tuotteessa ei säilötä henkilötietoja DNN-puolelle.

Siirtoformaatiksi valittiin yleisesti käytössä oleva Extensible Markup Language (XML) -merkintäkieli. Tähän päädyttiin erityisesti, koska tuotteen käyttämässä tietokantasovelluksessa oli valmiina mahdollisuus ottaa hakutulokset ulos suoraan XML-muodossa. Tekniikka ei valitettavasti ole SQL-standardin mukainen, mutta useista tietokantatuotteista löytyy vastaava toteutus. Esimerkkikoodissa 1 on esitetty osa SQL-proseduuria, jolla tuotetaan XML-muotoinen tuloste kontaktin henkilötiedoista ja hänen osallistumisistaan eri tapahtumiin.

```
SELECT Kontakti.KontaktiID, Kontakti.Nimi, Tapahtuma.TapahtumaID, Tapah-
tuma.Nimi, Osallistuminen.Tila
FROM Kontakti
INNER JOIN Osallistuminen ON Osallistuminen.KontaktiID = Kontakti.KontaktiID
INNER JOIN Tapahtuma ON Osallistuminen.TapahtumaID = Osallistuminen.Tapahtu-
maID
WHERE Kontakti.KontaktiID = 123456
FOR XML AUTO
```

Esimerkkikoodi 1. XML-muotoisen hakutuloksen tuottaminen Microsoft SQL Server -tietokannassa.

Tämän ominaisuuden avulla siirtotiedoston sisällön kokoaminen voitiin tehdä kokonaan yhden SQL-proseduurin avulla ilman, että tietoja tarvitsee käsitellä ohjelmiston puolella. Ei pidetty kustannustehokkaana tehdä siirtotiedostosta kovin hienostunutta ennen kuin käytännön kautta selviää, pyytävätkö asiakkaat siltä erityisominaisuuksia. Esimerkiksi siirtoon tuotavien tietokenttien nimiä ei muutettu minkään standardin mukaiseksi.

Siirtotiedoston lataamiseen luotiin käyttöliittymä tuotteen ylläpitäjän kontaktinhallintamoduuliin ja peruskäyttäjän omien tietojen näkymään. Kaikki asiakkaat eivät omien tietojen näkymää vielä käytä. Päätettiin että kustannustehokkaampia ja vähemmän manuaalista työtä vaativia automatisoituja ratkaisuja tutkitaan vasta, kun selviää, tuleeko siirtotiedostojen pyytämisestä jatkossa yleistä kansanhuvia, joka tuottaa asiakkaille paljon työtä.

Toteutuksessa huolehdittiin myös ominaisuuden rajauksesta siten, että kulloinkin kirjautunut käyttäjä voi noutaa vain omat tietonsa eikä esimerkiksi välittämään muiden käyttäjien tunnistetta käyttöliittymäpuolelta. Hallintapuoli jätettiin tarkoituksella vielä hieman avoimemmaksi sallien se kaikille ylläpitäjille ja siihen tullaan toteuttamaan rajausasetuksia yksi kerrallaan kunkin omien käyttötarpeiden mukaisesti.

Joillakin asiakkailla on kokonaan muista poikkeavia tietosisältöjä, jotka todennäköisesti halutaan mukaan siirtotiedostoon myöhemmin. Näitä tullaan lisäämään tarvittaessa todennäköisesti ohjelmiston puolella esimerkiksi siten, että ohjelmisto yhdistää useita eri tietokantahakuja yhdeksi kattavaksi siirtotiedostoksi. Ohjelmistossa on käytäntönä ollut ylläpidon selkeyttämiseksi toteuttaa asiakaskohtaiset räätälöinnit lähdekoodissa eikä tietokantapuolella.

4.5 Oikeus tulla unohdetuksi

Tuotteeseen toteutettiin aikaisempaa kattavampi henkilötietojen ja niihin liittyvän henkilökohtaisen datan poistotoiminto. Tuotteen olemassa oleva kontaktien poisto oli rajoittunut käyttäjän deaktivoitiin ilman tietojen lopullista poistamista ilman käsityötä. Tietosuoja-asetuksen kannalta katsottiin tässä vaiheessa riittäväksi, että tiedot anonymisoidaan poistamalla kaikki merkittävät henkilön tunnistamiseen liittyvät tiedot kuten nimi- ja osoitetiedot.

Tuotteessa on kahdenlaisia käyttäjätunnuksia, joihin henkilötietoja liittyy: DotNetNuke -alustan käyttäjätunnuksia ja tuotteen kontakteja. Jotkut asiakkaat hyödyntävät molempia tarjotakseen ylläpitäjille laajempia tapoja hallita käyttöoikeuksia. Unohdus toteutettiin molemmille tyypeille erikseen, jotta voitaisiin esimerkiksi varmistaa, että järjestelmästä ei asiakkaan tarpeesta riippuen katoa tunnistettavissa olevia lokitietoja ennen kuin ne voidaan poistaa, vaikka henkilö olisikin unohdettu muiden käsittelytarpeiden osalta.

Unohdus-toiminnon suunnittelussa ilmeni monenlaisia ongelmia. Toiminnon perustarkoitus on, että rekisteröidyn henkilötietojen käsittely lopetetaan. Kuitenkin raportoinnin ja muiden toimintojen kannalta on oleellista, että tietyn verran kontaktin tietoja, vaikkakin anonymisoituna, löytyy järjestelmästä jatkossakin. Tämän vuoksi esimerkiksi järjestelmässä tähän asti olleen ”poistettu”-tilan käyttö osoittautui ongelmalliseksi, sillä suurin osa tuotteesta huomioi eri listauksissa vain aktiiviset käyttäjät. Lopulta todettiin, että tietojen anonymisointi poistamisen sijaan ratkaisisi ongelman tyydyttävästi useimpien asiakkaiden tarpeiden suhteen. Asetuksen kannalta merkittävää on, että henkilöä ei tiedoista voida enää tunnistaa.

Toinen ongelmallinen tilanne syntyy, kun rekisterinpitäjällä on esimerkiksi lakisääteinen velvollisuus säilyttää henkilötietoja tietyn aikaa. Tätä ei vielä ratkaistu lopullisesti, sillä käytäntö tulee vahvistumaan vasta, kun käydään läpi ensimmäinen käyttöönottoprojekti

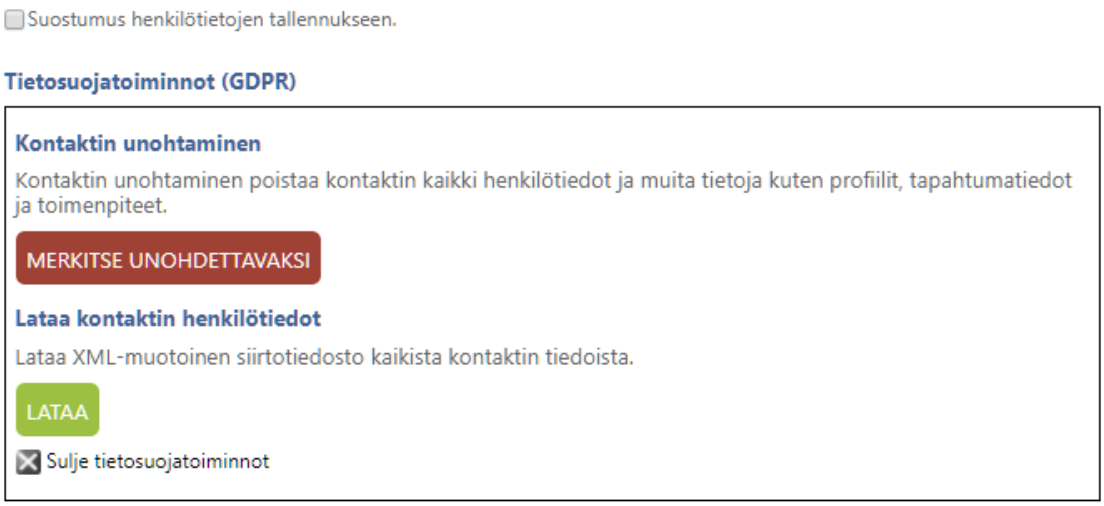
tällaista poikkeusta vaativalle asiakkaalle. Oletettavasti unohdustoimintoon tullaan vielä suunnittelemaan jonkinlainen ajastettava toiminto, jonka avulla henkilö unohdetaan pysyvästi vasta asiakaskohtaisesti määriteltävän ajanjakson jälkeen.

Kolmas merkittävä ongelma on asiakkaan ylläpitäjien järjestelmään dynaamisesti lisäämät kentät, jotka saattavat sisältää henkilötietoja. Näitä on vaikea ennakoida ja tietokannan täydellinen läpikäynti henkilötietojen löytämiseksi olisi epävarmaa. Päätettiin, että nämä tullaan käsittelemään erikseen niiden kanssa käyttöönottoprojekteissa, jotka dynaamisia kenttiä hyödyntävät. Todennäköisesti tietokantaproseduurit ohjelmoidaan poistamaan kaikki tiettyyn kontaktiin liittyvät dynaamiset tiedot, ellei asiakas ole tarkkaan määritellyt, mitä tietoja se kerää.

Poistamista varten luotiin tietokantaproseduureja jotka siivoavat tietokannasta kaikki haluttuun henkilöön liittyvät henkilötiedot. Asiakkailla on kuitenkin raportointitarpeita ja muita syitä, miksi osa henkilön liittyvistä tiedoista, kuten osallistumistiedot ja tapahtumapalauteet, haluttiin jättää paikoilleen. Henkilötietojen poiston jälkeen nämä tiedot kuitenkin ovat anonymisoitu eikä niitä enää voi liittää luonnolliseen henkilöön, joten ne voidaan jättää järjestelmään.

Tietojen anonymisoinnilla tuhoamisen sijaan haluttiin myös huolehtia tietokannan eheydestä. Tuotteen tietokantarakenne ei kaikilla asiakkailla varmista viite-eheyttä, joten tietueiden poistaminen saattaisi aiheuttaa ongelmia ohjelmiston toiminnassa. Toimintoa toteuttaessa mietittiin myös, että ohjelmistossa saattaa olla osia, joissa tietokantarelaatio on ohjelmistokoodissa pystytetty nyt anonymisoitavan henkilötiedon varaan. Toivottiin, että nämä tulevat esille viimeistään asiakaskohtaisessa testausvaiheessa, sillä ohjelmiston koon vuoksi niitä ei välttämättä vielä huomattu.

Unohduksen tietoja tuhoavan luonteen takia poistoprosessi tehtiin kaksivaiheiseksi: Ensin käyttäjä itse tai ylläpitäjä voi merkitä henkilön poistettavaksi. Poistetuksi merkittyä henkilöä ei enää voida käsitellä rutiininomaisesti, mutta hänet voidaan palauttaa aktiivisesti. Tällä haluttiin varmistaa, että käyttäjiä ei virheellisesti unohdeta. Tämän jälkeen riittävät käyttöoikeudet omaava ylläpitäjä voi suorittaa lopullisen unohdus-toiminnon. Kuva 6 esittelee ylläpitäjän GDPR-työkaluja ohjelmistossa.



Kuva 6. Ylläpitokäyttäjän käyttöliittymä tietosuoja-asetuksen toimintoihin.

Rekisteröidyille toteutettiin samankaltaiset toiminnot unohdusta varten ohjelmistossa jo ennestään olleeseen Omat tiedot -moduulin. Käyttäjä voi pyytää tietojensa unohdusta, mutta vasta ylläpitäjä voi vahvistaa pyynnön.

Työtä tehtäessä todettiin, että myös tietokannan varmuuskopiot ovat henkilöstörekistereitä ja unohduksen pitää periaatteessa ulottua myös niihin. Kuitenkin käytettävyyden turvaamiseksi varmuuskopioista ei voida helposti luopua. Koska ne on säilytty turvasäiliöön sijoitetuille massamedioille, niin unohduksen ulottaminen niihin asti olisi erittäin hankalaa ilman manuaalista työtä. Tietosuoja-asetus kuitenkin sisältää jonkin verran liikkumavaraa. Esimerkiksi 25. artikla [Asetus 2016/679 2016: 48] toteaa oletusarvoisesta tietosuojasta puhuessaan, että toteutusta pohdittaessa huomioidaan riskien taso, käytössä oleva tekniikka ja toteuttamiskustannukset. Näiden valossa todettiin, että työtä varmuuskopioon tallennetun unohduksen toteuttamiseksi ei vielä aloiteta vaan odotetaan Unionin valmistelutyöryhmien ohjeistusta asiaan liittyen. Varmuuskopiokysymys kuitenkin on ajankohtainen kaikille yrityksen rekisterinpitäjäasiakkaille, joten sitä tullaan seuraamaan, kunnes yrityksellä on tarjottavana ratkaisuehdotuksia asiakkailleen.

Toiminnon toteutus oli jo valmistunut, kun huomattiin, että eri asiakkaiden tietokannoissa oli tauluja ja sarakkeita, joita muilla ei ollut. Asiakaskohtaiset tietokantataulut oli helppo kiertää ohjelmoimalla tietokantaproseduurit ajamaan toimenpiteet vain, jos kukin taulu oikeasti löytyy. Puuttuvien sarakkeiden osalta tällainen olisi ollut huomattavasti haastavampaa. Lopulta päätettiin, että tietokantarakenteet tullaan yhdistämään sarakkeiden

osalta, vaikka se tarkoittaisikin ylimääräisiä käyttämättömiä sarakkeita joissain tietokannoissa.

5 Yhteenveto

Opinnäytetyön tavoitteena oli selvittää, mitä toimia EU:n tietosuoja-asetuksen 697/2016 vaatimustenmukaisuuden tavoittaminen vaatii työn tilanneen yrityksen toiminnassa ja ohjelmistotuotteissa ja auttaa sen saavuttamisessa erityisesti teknisellä puolella. Olin aloittanut työsuhteen työn tilaajaan muutamaa kuukautta aikaisemmin, joten tilaajan käytännöt ja toimintaympäristö eivät ennestään olleet kovin tuttuja.

Aloitin tutustumisen aiheeseen lukemalla itse asetuksen ja etsimällä Internetistä materiaalia. Erityisesti Valtiovarainministeriön Vahti-työryhmän tekemä raportti oli suurena apuna aiheen jäsentelyssä. Konkreettisia toteutusohjeita asetuksen toteuttamisesta käytännöstä oli vaikea löytää, vaikka useat lähteet kertoivatkin että sekä maakohtaiset että koko Euroopan unionin kattavat viranomaiselimet olisivat niitä tuottamassa. Aikaisempaa omakohtaista kokemusta tietosuoja-asetuksesta tai kovin tarkkaa kuvaa Suomen aiemmasta henkilötietolaista minulla ei ollut.

Suurin haaste oli asetuksen koko laajuuden omaksuminen ja tilaajayrityksen nykytilan peilaaminen siihen. Vahti-työryhmän tekemät työkalut auttoivat käsittelyn aloittamisessa huomattavasti ja niiden avulla pystyttiin paremmin kohdistamaan opinnäytetyön puitteissa toimitettava toteutus ohjelmistoteknisiin muutoksiin. Työlle alun perin suunniteltu laajuus supistui sen kuluessa, ja yrityksen johto osallistui konkreettisesti erityisesti hallinnollisten tietoturva-asioiden suunnitteluun.

Toinen suuri haaste työn laadukkaalle toteutumiselle oli järjestää työaikaa sitä varten. Muiden työtehtävien suuri määrä vähensi opinnäytetyöhön liittyviin tehtäviin käytettävissä ollutta työaikaa.

Olen itse hieman pettynyt, että työtä jouduttiin rajaamaan ja mielenkiintoiset asiat kuten yrityksen ohjelmistotuotteen tietoturva- ja suojatason analysointi ja parantaminen jäivät tässä työssä vähemmälle huomiolle. Totesimme työn loppuvaiheessa, että asetus kokonaisuudessaan on niin suuri kuvio, että parempi ottaa yksi askel kerrallaan, jotta ei la-

maannu työmäärän edessä. Sekä tilaaja että minä olemme iloisia, että tietosuoja-asetuksen valmistelutyö on nyt päässyt vauhtiin näkyvästi ja konkreettisesi ja että useita jatkotoimenpiteitä on jo suunniteltu.

Tietosuoja-asetuksen siirtymäajasta on enää neljännes jäljellä mutta valmistelutyötä tehdään varmaan monissa yrityksissä vielä sen päätyttyäkin ja jokaisessa uudessa henkilötietoja sivuavassa ohjelmistoprojektissa. Olen varma, että pystyn hyödyntämään opinnäytetyön aikana kerättyä tietoa työssäni jatkossakin.

Lähteet

Asetus 2016/679. 2016. Euroopan parlamentti ja neuvosto. Verkkodokumentti. <http://eur-lex.europa.eu/legal-content/fi/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Julkaistu 4.5.2016. Luettu 15.6.2017.

Chaturvedi, Aditi. 2017. Comparison of General Data Protection Regulation and Data Protection Directive. Verkkodokumentti. <https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive>. Julkaistu 7.2.2017. Luettu 17.8.2017.

Commission decisions on the adequacy of the protection of personal data in third countries. 2017. Verkkodokumentti. <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Luettu 28.8.2017.

Forni, Amy Ann & van der Meulen, Rob. Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation. Verkkodokumentti. <http://www.gartner.com/newsroom/id/3701117>. Julkaistu 3.5.2017. Luettu 14.7.2017.

Freeman, Rob. 2017. The GDPR and data protection impact assessments (DPIA) – why are they required?. Verkkodokumentti. <https://www.itgovernance.co.uk/blog/the-gdpr-and-data-protection-impact-assessments-dpia-why-are-they-required/>. Julkaistu 29.3.2017. Luettu 22.10.2017.

Nevala, Meri-Tuuli. 2017. Nyt puhuttaa GDPR eli EU:n tietosuoja-asetus. Verkkodokumentti. <https://www.havain.fi/nyt-puhuttaa-gdpr-eu-tietosuoja-asetus/>. Julkaistu 10.5.2017. Luettu 17.8.2017.

Nevasalo, Terho; Tenhunen, Sami. 2017. HPP Asianajotoimisto. GDPR Ready 2018 - Osa V Perusteet haltuun. Luentomoniste. <http://www.gdpr.fi/materiaalit/9-12-23-5-gdpr-ready-2018-perusteet-haltuun-materiaalit/>. Julkaistu 23.5.2017. Luettu 25.5.2017.

Nurmi, Pekka; Talus, Anu; Jaatinen, Tanja; Hänninen, Anna; Rankalankila, Leena; Vettenranta, Leena. 2017. Oikeusministeriö. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Verkkodokumentti. <http://urn.fi/URN:ISBN:978-952-259-612-3>. Julkaistu 21.6.2017. Luettu 19.8.2017.

Privacy Shield Program Overview. 2017. U.S. Department of Commerce. Verkkodokumentti. <https://www.privacyshield.gov/Program-Overview>. Luettu 29.8.2017.

VAHTI-raportti 1/2016 EU-tietosuojan kokonaisuudistus. 2016. Valtiovarainministeriö. Verkkodokumentti. <http://urn.fi/URN:ISBN:978-952-251-778-4>. Julkaistu 2.6.2016. Luettu 15.6.2017.