LAPIN AMK
Lapland University of Applied Sciences

HENKILÖTIETOJEN KÄSITTELY ASIAKASPALVELUN NÄKÖKULMASTA ENONTEKIÖN SÄHKÖ OY:SSÄ

Palojärvi Hanna Maaren

Opinnäytetyö

Liiketalouden koulutus
Tradenomi AMK

2021

Liiketalouden koulutus
Tradenomi

Tekijä Hanna Maaren Palojärvi Vuosi 2021
Ohjaaja Tia Lämsä
Toimeksiantaja Enontekiön Sähkö Oy
Työn nimi Henkilötietojen käsittely asiakaspalvelun näkökulmasta Enontekiön Sähkö Oy:ssä
Sivu- ja liitesivumäärä 56 + 9

Opinnäytetyössä kuvattiin asiakaspalvelijan näkökulmasta ja muistilistan tyylisesti henkilötietojen käsittelyä sekä niihin liittyviä tietosuoja- ja tietoturvariskejä. Opinnäytetyö tehtiin Enontekiön Sähkö Oy:n henkilötietojen käsittelyn tueksi ja mahdollisten parannustarpeiden huomaamiseksi. Työn liitteenä on päivitetty tietosuojaseloste sekä pieni muistilistamainen ohje henkilötietojen käsittelijälle.

Opinnäytetyön tutkimusote oli laadullinen, jossa oli mukana oikeusdogmatiikan vivahteita. Empiirisen tiedon hankkimiseksi ja asiakaspalvelijan näkökulman avaamiseksi opinnäytetyöhön haastateltiin henkilötietojen käsittelijöitä. Haastattelut toteutettiin teemahaastatteluina. Haastattelujen avulla teorian tueksi saatiin käytännön esimerkkejä ja työelämän antamaa kokemusta tietosuojasta ja tietoturvasta.

Teoriaosuuden pääpaino oli Euroopan unionin tietosuoja-asetuksessa sekä Suomen lainsäädännössä. Alan tietokirjallisuutta hyödynnettiin siten, että tietojen tuli olla uusia tietosuoja-asetuksen käyttöönottamisen jälkeen julkaistuja tietoja. Työn ulkopuolelle on rajattu organisaation henkilökunnan henkilötietojen käsittely, koska opinnäytetyön ei haluttu laajenevan työelämälainsäädäntöön.

Opinnäytetyössä kuvattiin henkilötietojen käsittelyä niin rekisterinpitäjän kuin rekisteröidynkin näkökulmasta. Olennaisessa roolissa työssä on henkilötietojen käsittelijä, jonka tulee tietää laaja-alaisesti ja kokonaisuutena henkilötietojen käsittelyprosessi. Työ sopii luettavaksi hyvin uudelle työntekijälle, jolle käytännöt voivat olla vielä vieraita. Työtä voidaan kokonaisuudessa ajatella myös muistilistana, johon voidaan palata uudelleen tarpeen tullen työn ohessa. Pohdinnassa on keskitytty Enontekiön Sähkö Oy:n henkilötietojen käsittelyn nykytilaan ja esitetty parannusehdotuksia käsittelyyn siihen liittyvien riskien minimoimiseksi. Pohdinnassa mietitään myös henkilötietojen käsittelijän suurta vastuuta tietojen elinkaaren hallinnassa.

Avainsanat Asiakastietojärjestelmä, henkilötieto, tietosuoja, tietoturva, riskienhallinta, henkilötietojen käsittelijä, rekisteröity, rekisterinpitäjä

Degree Programme in Business Administration
Bachelor of Business Administrtion

Author	Hanna Maaren Palojärvi	Year	2021
Supervisor	Tia Lämsä		
Commissioned by	Enontekiön Sähkö Oy		
Subject of thesis	Personal data processing from the view of customer service in Enontekiön Sähkö Oy		
Number of pages	56 + 9		

The thesis described the processing of personal data from the perspective of a customer service representative, as well as the related data protection and security risks. The thesis was done in the style of a checklist to support the processing of Enontekiön Sähkö Oy`s personal data and to notice possible needs for improvement. An updated Privacy Statement and a checklist guide for the personal data processor are attached to the thesis.

The research approach of the thesis was qualitative, which includes nuances of legal dogmatics. In order to obtain empirical information and open the perspective of the customer service representative to the thesis, personal data processors were interviewed. The interviews were conducted with thematic interviews. The interviews provided practical examples to support the theory and the experience of working life in data protection and security.

The main focus of the theoretical part was on the European Union's data protection regulation and Finnish legislation. The literature in the field published since the introduction of the Data Protection Regulation has been used. The processing of personal data of the organisation´s staff has been excluded from the work, because the thesis was not intended to be extended to working life legislation.

The thesis examines the processing of personal data from the perspective of both the registrar and the data subject. An essential role in the work is played by the person processing of personal data, who must know the personal data processing process extensively and as a whole. The work is well suited to be read by a new employee for whom the practices may still be unfamiliar. The work as a whole can also be thought of as a checklist, which can be reviewed when needed.
The discussion has focused on the current state of Enontekiön Sähkö Oy's processing of personal data and proposed improvements to the personal data processing in order to minimize the related risks. The discussion underlines also the great responsibility of the data controller in managing the personal data lifecycle.

Key words: Customer information system, personal data, data protection, data security, risk management, personal data processor, registered, data controller

SISÄLLYS

1 JOHDANTO 6

1.1 Tutkimuksesta 6
1.2 Tutkimusmenetelmä 7

2 HENKILÖTIETOJEN KÄSITTELYN NYKYTILA-ANALYYSI 10

2.1 Käsittelyn nykytila 10
2.2 Henkilötietojen säilytys 10
2.3 Henkilötietojen kerääminen 12
2.4 Käyttöpaikan ja liittymän tunnistetiedot 13

3 ASIAKASTIETOJEN PÄIVITTÄMINEN 15

3.1 EnerimCIS-asiakastietojärjestelmän käyttöönotto 15
3.2 Datahub – keskitetyn tiedonvaihdon kanava 16
3.3 Henkilötietojen päivittämisen prosessi 16
3.4 Henkilötietojen käsittelijän kokemus 18

4 REKISTERINPITÄJÄ JA HENKILÖTIETOJEN KÄSITTELIJÄ 21

4.1 Rekisterinpitäjä 21
4.2 Omavalvontasuunnitelma 21
4.3 Henkilötietojen käsittelijä 22
4.4 Sähkömarkkinoiden tiedonvaihto 23
4.5 Tietojen luovuttaminen 24
4.6 Käsittelyn läpinäkyvyys ja osoitusvelvollisuus 27
4.7 Tietosuojaseloste 29
4.8 Seloste käsittelytoimista 30

5 REKISTERÖIDYN OIKEUDET 31

5.1 Oikeudet tietosuoja-asetuksessa 31
5.2 Lokitiedot 33
5.3 Tietojen tarkastuspyyntö 33

6 TIETOSUOJARISKIT 35

6.1 Tietosuojasta 35
6.2 Riskien arviointi 36
6.3 Riskienhallintastandardit 37

7 TIETOTURVARISKIT 38
7.1 Tietoturvasta 38
7.2 Työskenneltäessä huomioitavaa 39
7.3 Kyberturvallisuus 41
8 HENKILÖTIETOJEN KÄSITTELY 43
8.1 Huolellisuusvelvoite 43
8.2 Asiakaspalvelutilanne 43
8.3 Vaitiolovelvollisuus 45
8.4 Käyttö- ja salassapitositoumus 46
9 HENKILÖTIETOJEN KÄSITTELY KENTTÄTYÖSSÄ 48
10 POHDINTA 50
LÄHTEET 52
LIITTEET 56

1 JOHDANTO

1.1 Tutkimuksesta

Henkilötietojen käsittelyä tehdään tällä hetkellä enemmän kuin koskaan ennen. Lisääntyneen käsittelyn myötä rekisterin pitäjällä, henkilötietojen käsittelijällä ja rekisteröidyllä on lisääntyneet myös lain asettamat oikeudet ja velvoitteet. Opinnäytetyössä käyn läpi asiakaspalvelijan tekemää henkilötietojen keräämistä ja päivittämistä riskienhallinnan näkökulmasta. Tutkimusongelmana on henkilötietojen käsittely Enontekiön Sähkö Oy:ssä. Tutkimuskysymyksenä on, miten Enontekiön Sähkö Oy:ssä käsitellään henkilötietoja ja kuinka siihen liittyvät riskit on huomioitu. Apututkimuskysymyksiä ovat, mitkä ovat henkilötietojen keräämistä ja päivittämistä koskevat ongelmat, lait, velvollisuudet ja oikeudet. Minkälaisia riskejä henkilötietojen käsittelyssä on? Miten tietoturva on otettu huomioon?

Enontekiön Sähkö Oy on verkkopalveluyhtiö, joka palvelee asiakkaitaan Enontekiön kunnan alueella, yhtiöllä on noin 1800 asiakasta. Verkkopalveluyhtiö tarvitsee erinäisiä tietoja asiakkaasta, sähkönkäyttöpaikasta, verkkopalvelusopimuksesta, käyttöpaikan sähkönkulutuksesta ja sähköliittymästä. Yhtiö kerää siis paljon asiakkaan henkilötietoja, joihin lukeutuvat myös sähkönkäyttöpaikkaa koskevat tiedot. Opinnäytetyössä perehdytään Enontekiön Sähkö Oy:n henkilötietojen käsittelyyn käyttäen apuna kahta meneillään olevaa isoa projektia, joissa molemmissa on keskiössä henkilötiedot ja niiden käsittely. Henkilötietojen käsittely nousi yhtiössä esille näiden projektien myötä ennenkokemattomalla tavalla, koska yhtäkkiä koko asiakasdata tuli käydä huolellisesti läpi.

Opinnäytetyössä tutkitaan pääsääntöisesti Euroopan unionin vuonna 2016 voimaan tullutta tietosuoja-asetusta (EU) 2016/679. Tietoperustaa haetaan myös kotimaisesta lainsäädännöstä sekä alan kirjallisuudesta. Opinnäytetyön ulkopuolelle rajataan henkilöstön henkilötietojen käsittely, koska opinnäytetyötä ei haluta laajentaa työelämälainsäädäntöön.

Opinnäytetyön tarkoituksena on antaa lakikatsaus sekä tietoa Enontekiön Sähkö Oy:n henkilökunnalle henkilötietojen käsittelystä. Tarkoituksena on, että työntekijöille muistuu mieleen tietosuojan ja tietoturvallisuuden tärkeys työelämässä. Opinnäytetyö on myös hyödyllinen uusille työntekijöille, joille tietosuojaan liittyvät asiat voivat olla vielä haasteellisia. Opinnäytetyön tuotoksena on päivitetty tietosuojaseloste sekä lyhyt muistilista työntekijöille henkilötietojen käsittelystä (Liite 3.).

Euroopan unionin tietosuojalainsäädännön uudistaminen aloitettiin vuonna 2012, koska lainsäädäntö oli jäänyt kehityksestä jälkeen eikä enää vastannut maailmanlaajuisia toimintamalleja ja olosuhteita. Uudistuksen tavoitteena oli tehdä henkilötietojen suojasta perusoikeus, kehittää digitaalitaloutta, torjua terrorismia ja rikollisuutta. Yleinen tietosuoja-asetus, englanniksi General Data Protection Regulation, on asetus, josta laajasti käytetään lyhennettä GDPR. Tietosuoja-asetus edellytti Suomen henkilötietolainsäädännön tarkistamista, minkä tuloksena säädettiin uusi tietosuojalaki, joka toimii henkilötietojen käsittelyssä yleislakina. Tietosuoja-asetus astui voimaan vuonna 2016, ja sitä alettiin soveltamaan jäsenvaltioissa vuonna 2018. Asetusta sovelletaan sekä julkisella että yksityisellä sektorilla. (Bergström, Karhula & Kipinoinen 2018.)

Euroopan unionin tietosuoja-asetus on merkityksellinen yksilön suojelun ja henkilötietojen käsittelyn kannalta. Se yhdenmukaistaa jäsenvaltioiden tavan ja tuo henkilötietojen suojan samalle tasolle sekä yhdenmukaistaa EU:n digitaalisen sisämarkkinan säännöksiä, toimintatapoja ja -edellytyksiä. Yrityksille asetus antaa mahdollisuuden parantaa omaa tietojenhallintaansa ja antaa mahdollisuuden laajentua koko Euroopan alueelle, koska kun vaatimukset tietojen hallinnasta täyttyvät yhdessä jäsenvaltiossa, ne täyttyvät muissakin. (Aalto-Setälä & Viitaila 2018.)

1.2 Tutkimusmenetelmä

Tutkimusote opinnäytetyössä on laadullinen, jossa on mukana myös muita tutkimusotteita. Koska kyseessä on toiminnallinen projekti, jossa ihmisen omalla kokemuksella on merkitystä, tutkimusmenetelmässä on mukana myös empiirisen tutkimuksen piirteitä. Empiirinen tieto koskee kokemukseen perustuvaa tietoa, ja tässä opinnäytetyössä tätä tietoa antavat haastattelut (Juuti & Puusa 2020).

Havaintoaineiston pienuuden (viisi haastateltavaa) vuoksi kvantitatiivista eli määrällistä analyysia ei ole suoritettu eikä aineiston perustella näin ollen voida tehdä yleistyksiä. Tiedon intressi tässä opinnäytetyössä on pragmaattinen, ja saatua tietoa pyritään jatkossa käyttämään tutkittavan organisaation kehittämiseen. (Hirvonen 2011). Opinnäytetyössä tutkitaan myös jonkin verran lainoppia eli mukana on myös oikeusdogmatiikan vivahteita.

Laadullisella tutkimuksella halutaan ymmärtää tarkasteltavan ilmiön kohteena olevien henkilöiden näkökulmaa. Tässä työssä tuo näkökulma on asiakaspalvelijan. Opinnäytetyössä ollaan kiinnostuneita asiakaspalvelijoiden kokemuksista laadullisen tutkimuksen näkökulmasta ja henkilötietojen käsittelystä oikeusdogmatiikan näkökulmasta. Teoria on keskeisessä osassa laadullista tutkimusta, ja tutkimuksessa teoria ja haastattelut ovat vuoropuhelussa. Teoria toimii aineistonkeruun perustana laadullisessa tutkimuksessa. (Juuti & Puusa 2020.)

Lainoppi eli oikeusdogmatiikka näkyy työssä siten, että siinä on tutkimuksen kohteena voimassa olevat lait ja asetukset. Kokonaan ei voida kuitenkaan puhua oikeusdogmatiikan tutkimusmenetelmästä, koska työssä ei tulkita lakeja, vaan viitataan niihin työelämä lähtöisesti ja pohditaan, mitä lakia tulee kulloinkin noudattaa. Opinnäytetyössä on käytetty paljon vahvasti velvoittavia eli legalisoituja oikeuslähteitä. Opinnäytetyössä ei ole käsitelty lakien esitöitä tai ennakkoratkaisuja. (Nykänen 2019.)

Empiirisen tiedon saamiseksi opinnäytetyöhön on haastateltu verkkopalveluyhtiöissä palvelevia henkilötietojen käsittelijöitä ja sähköverkkoasentajia. Opinnäytetyöhön haastateltiin yhteensä viittä henkilöä. Toisen verkkopalveluyhtiön mukaan ottaminen haastatteluun oli pakollista, koska Enontekiön Sähkö Oy:n organisaatio on pieni, ja vain kaksi henkilöä tekee päivittäin töitä, joihin kuuluu asiakaspalvelua ja henkilötietojen käsittelyä. Myös tutkimuseettisistä syistä toisen organisaation mukaan ottaminen oli välttämätöntä, jotta henkilöiden tunnistaminen ei olisi aivan niin ilmeistä. Toinen verkkopalveluyhtiö, joka otettiin mukaan tähän tutkimukseen, on hyvin samankaltainen kuin Enontekiön Sähkö Oy. Datahub ja asiakastietojärjestelmäprojektit olivat myös kyseisessä yhtiössä yhtäaikaisesti käynnissä Enontekiön Sähkö Oy:n projektien kanssa. Haastateltaviin kuului myös

sähköverkkoasentajia, jotta saatiin näkemystä myös heidän henkilötietojen käsittelyn tilasta, tarpeesta ja käsittelytavoista.

Haastattelut toteutettiin teemahaastatteluina pareittain ja yksilöittäin. Teemahaastattelu on yleisimmin käytetty haastattelumuoto, jossa tutkimusongelmasta poimitaan keskeisimmät aiheet (Vilkka 2015, 124). Haastattelukysymykset ovat opinnäytetyön liitteenä (Liite 1.). Haastattelussa kysymykset toimivat haastattelijan tukena ja keskustelun runkona ja johdattelijana. Haastatteluja ei käyty kysymysten mukaisessa järjestyksessä, vaan vapaasti järjestystä muutellen.

Eettisesti arvioiden työ oli hyvin tavallinen laadullinen tutkimus, jossa ei käsitelty kenenkään ihmisen henkilötietoja, vaan niistä puhuttiin lakien ja haastattelujen kautta. Hyvän tutkimuskäytännön mukaisesti haastateltavilta saatiin tutkimukseen osallistumisesta suostumus joko sähköpostitse tai suullisesti. Haastateltaville kerrottiin, mihin tarkoitukseen haastatteluaineistoa käytettäisiin ja, että haastattelumateriaali tuhottaisiin heti sen tarpeellisuuden päätyttyä. Haastateltavat esiintyivät opinnäytetyössä anonyymeinä. Opinnäytetyön teoriaosuudessa on noudatettu hyvän tieteellisen kirjoittamisen periaatteita ja viittauskäytänteitä. Opinnäytetyötä varten on tehty opinnäytetyösopimus. Opinnäytetyön ohjaaja hyväksyi haastattelukysymykset ennen haastattelun aloittamista. (Tutkimuseettinen neuvottelukunta 2012.)

Opinnäytetyön luotettavuutta voidaan arvioida esimerkiksi siten, että tutkitaan onko lähdeaineisona käytetty alan tuoreinta tietokirjallisuutta, Suomen lainsäädäntöä sekä Euroopan unionin tietosuoja-asetusta. Näin on tehty. Haastatteluissa esille nousseita asioita on pyritty reflektoimaan eli peilaamaan tematiikkaa sitä koskeviin lakeihin tai teoriaan. Opinnäytetyö ei tarjoa objektiivista tai absoluuttista tietoa, vaan opinnäytetyö on kontekstuaalinen tekijäänsä sekä aiheen lähestymistapaan nähden. (Saaranen-Kauppinen & Puusniekka 2006).

2 HENKILÖTIETOJEN KÄSITTELYN NYKYTILA-ANALYYSI

2.1 Käsittelyn nykytila

Henkilötietojen käsittelyä yhtiössä kannattaa lähteä arvioimaan tekemällä henkilötietojen nykytila-analyysin. Analyysin avulla tunnistetaan, miten ja minkälaisia henkilötietoja yhtiössä käsitellään, missä ja kuinka kauan niitä säilytetään, kuka niitä käsittelee, kuinka kauan henkilötietoja säilytetään sekä kuinka ne hävitetään. Nykytila-analyysissä tehdään henkilötietoinventaario sekä henkilötietojen elinkaarihallintaa. (Aalto-Setälä & Viitaila 2018, 37.)

Enontekiön Sähkö Oy verkkopalveluyhtiönä tarvitsee asiakkaistaan paljon erilaisia henkilötietoja liittymä- ja verkkopalvelusopimusten tekemiseen. Yhtiön tarvitsemat henkilötiedot ovat nimi, henkilötunnus, osoitetiedot, puhelinnumero, sähköpostosoite, mahdollinen laskutusosoite sekä käyttöpaikan tiedot.

Käyttöpaikan tiedoilla tarkoitetaan sähkön käyttöpaikan identifioivia tietoja. Näitä ovat käyttöpaikan osoite, sähköliittymän sulakekoko sekä sähkömittarin tiedot kuten mittarin malli ja numero. Nämä tiedot saamme omista järjestelmistämme, emme asiakkaalta. Kun asiakkaan kanssa on tehty verkkopalvelusopimus tai pientuotantosopimus, saadaan käyttöpaikalta lisää tietoja, jotka voidaan lukea mukaan henkilötiedoiksi. Sähkönkäyttöpaikalle tulee mittari, jonka malli ja numero antavat tiedon kenen mittarista on kysymys. Lisäksi ne myös mittaavat käyttöpaikalla kulutettua tai tuotettua sähköä, ja tämä luetaan myös henkilötiedoksi. Henkilötiedoksi luetaan kaikki tiedot, joilla rekisteröity voidaan tunnistaa suoraan tai epäsuorasti. (EU:n tietosuoja-asetus 4 artikla 1 kohta.)

2.2 Henkilötietojen säilytys

Enontekiön Sähkö Oy:llä henkilötietoja on useassa eri järjestelmässä, koska nykyteknologia vaatii useiden erilaisten yhtäaikaisten tietojärjestelmien käytön. Yhtiön keräämiä asiakastietoja on nykyhetkellä kuudessa erilaisessa tietojärjestelmässä, joita ovat CRM- asiakastietojärjestelmä, AX-laskutusjärjestelmä, Generis-mittaustieto- ja käyttöpaikkajärjestelmä, Online-palvelu, Mitello-jakeluverkon kunnossapito ohjelma sekä Telian kulutusmittauspalvelu. Asiakastietoja on myös

Enontekiön kunnan arkistossa, johon arkistoidaan liittymäsopimukset Arkistolain 23.9.1994/831 mukaisesti. Liittymäsopimukset ovat myös sähköisessä muodossa Enontekiön kunnan suojatulla verkkopalvelimella.

Yhtiössä henkilötietoja käsittelee pääsääntöisesti vain kaksi henkilöä pienen organisaation takia. Sähköverkkoasentajat käsittelevät vain joissain määrin henkilötietoja, joten tietojen käsittely ei heille ole päivittäistä. Tilanteet, joissa sähköverkkoasentaja käsittelee henkilötietoja, ovat esimerkiksi sähkönkäyttöpaikalla ilmennyt vikatilanne, uuden tai purettavan sähköliittymän käsittely sekä sähkön kytkentätoimeksiannot sähkökäyttöpaikalla. Näissä tilanteissa sähköverkkoasentaja käsittelee vain välttämättömiä henkilötietoja sekä tietoja, joista asiakas on välillisesti tunnistettavissa, kuten käyttöpaikannumero.

Asiakastietoja ja erinäisiä sopimuksia yhtiössä säilytetään 10 vuotta sopimuksen päättymisen jälkeen (Kirjapitolaki 30.12.1997/1336 10§). Asiakaspalvelun puhelintallenteet säilytetään kaksi vuotta, jonka jälkeen ne hävitetään palveluntarjoajan toimesta automaattisesti. Asiakirjat sekä muut kirjallisessa muodossa olevat henkilötiedot kerätään hävitystä varten lukollisiin keräysastioihin, ja ne tuhotaan ostopalveluna. Muistilaput, joihin asiakaspalvelutilanteen aikana on, saatettu kirjoittaa muistiin asiakkuutta koskevia tietoja on myös hävitettävä laittamalla ne keräysastioihin. Henkilötiedot hävitetään poistamalla asiakkaan tiedot ohjelmista palveluntarjoajan avustuksella. Valitettavasti yhdessäkään ohjelmassa ei ole olemassa automatiikkaa, joka nostaisi poistettavan asiakkaan automaattisesti esille.

Keväällä 2021 käyttöön otettavaan EnerimCIS-asiakastietojärjestelmään annettiin tätä automatiikkaa koskeva kehitysidea. Prosessissa ohjelma hakisi taustaajoina poistettavia asiakastietoja. Tämä ehdotus annettiin koulutustilaisuudessa EnerimCIS-asiakastietojärjestelmän tuottajalle Empowerille. Tällä hetkellä vielä henkilötietojen käsittelijän on huomattava, milloin asiakastiedosta on tullut säilytysajan täytyttyä tarpeeton ja poistettava tieto manuaalisesti.

2.3 Henkilötietojen kerääminen

Enontekiön Sähkö Oy kerää ja käsittelee henkilötietoja asiakassuhteiden ja sähkönkäyttöpaikkojen hoitamista varten. Henkilötietojen käsittely on perusteltua rekisterinpitäjän toiminnan kannalta, koska verkkopalvelusopimuksen tekeminen on niin sanottu velkasuhde. Sopimuksia, joissa sitoudutaan maksamaan hyödyke myöhemmin, pidetään velkaantumisena eli velkasuhteena (Kuluttajaliitto 2017, 3. EU:n tietosuoja-asetus 5 artikla alakohta b.)

Henkilötiedot kerätään asiakkailta ensisijaisesti asiakassuhteen alussa, eli siinä vaiheessa, kun asiakkaan kanssa tehdään verkkopalvelu-, liittymä- tai pientuotantosopimus. Asiakkaalta kerään ainoastaan sellaiset välttämättömät tiedot, jotka asiakkuuden hoitaminen vaatii. Henkilötietoja saa käyttää ainoastaan käyttötarkoitussidonnaisesti asiakassuhteiden ja sähkönkäyttöpaikkojen hoitamista varten. (EU:n tietosuoja-asetus, 5 artikla.)

Käyttötarkoitussidonnaisia tietoja ovat nimi, henkilötunnus, osoite, mahdollinen laskutusosoite, puhelinnumero ja sähköpostiosoite. Verkkopalvelumaksujen ja liittymähinnan palautusta varten yhtiö joutuu kysymään asiakkaalta tilinumeroa ja pankkia, jotta palautus voidaan suorittaa asiakkaalle. Näistä edellä mainituista tiedoista henkilötunnus on poikkeuksellisen tärkeä henkilötieto, jonka avulla asiakas tunnistetaan esimerkiksi asiakaspalvelutilanteessa. Henkilötunnusta saa käsitellä, jos se on rekisteröidyn yksilöimisen kannalta tärkeää. Verkkopalvelusopimuksen ollessa velkasuhde henkilötunnusta verkkopalveluyhtiö saa käsitellä myös siksi, koska kyse on luotonannosta ja vakuustoiminnasta. (Tietosuojalaki 5.12.2018/1050 29§.)

Sähkömarkkinalaissa on säädetty, että henkilötunnusta voidaan käyttää henkilön tunnistamiseksi sähkönkaupan tiedonvaihdossa. Sähköalan yritys saa käsitellä henkilötunnusta sähkömarkkinalain säätämien tehtävien ja velvollisuuksien suorittamiseksi ja täyttämiseksi. (Sähkömarkkinalaki 9.8.2013/588, 75 d§.)

Minkäänlaisia erityisiä henkilötietoja eli arkaluonteisia tietoja yhtiö ei kerää missään tilanteessa asiakkaistaan. Arkaluontoisiksi tiedoiksi luokitellaan sellaiset tiedot, jotka ovat rekisteröidyn perusoikeuksien sekä vapauksien kannalta arkaluontoisia, näitä tietoja ovat esimerkiksi etnisyys ja uskonnollinen vakaumus. (EU:n

Tietosuoja-asetus 9 artikla). Tietoja asiakkaasta minimoidaan, koska pyydettävien tietojen tulee olla yhtiön toiminnan kannalta oleellisia ja asianmukaisia. Suhde käsittelyyn tulee olla tarkoituksenmukainen. (EU:n Tietosuoja-asetus 5 artikla c alakohta). Tietoja määrä minimoidaan myös siksi, ettei asiakasdata paisuisi kovin suureksi. Suurien datamäärien käsittely on raskasta ja vie paljon kapasiteettia tietojärjestelmistä. Suurien datamassojen alla myös oleellinen tieto on huonommin saatavilla.

Asiakastietojärjestelmän muistiinpanokenttään voidaan asiakkuudesta kirjoittaa tärkeitä tietoja. Tällainen muistiinpano voisi olla vaikkapa asiakkaan tilinumero verkkopalvelumaksujen palautusta varten, koska tilinumerolle ei ole nykyisessä asiakastietojärjestelmässä omaa kohtaa. Asiakaspalvelijan eli henkilötietojen käsittelijän tulee kuitenkin käyttää vahvasti omaa harkintaansa ja tietotaitoansa siinä, että hän itse ymmärtää, minkälaista tietoa muistiinpanokenttään saa ja ei saa laittaa. Minkäänlaista asiakasta kuvaavaa tietoa kenttään ei tule kirjoittaa. Tällainen kuvaava tieto voisi olla vaikkapa asiakkaan terveydellistä tilaa tai asiakkaan käyttäytymistä asiakastilanteessa kuvaava ilmaisu.

2.4 Käyttöpaikan ja liittymän tunnistetiedot

Muuttotilanteessa asiakkaalta kysytään käyttöpaikan osoite, jonka jälkeen asiakaspalvelija löytää käyttöpaikan tiedot asiakastietojärjestelmästä. Henkilön muuttaessa käyttöpaikan tunnistetiedot tulevat asiakkaan henkilötiedoiksi, koska niistä voidaan epäsuorasti tunnistaa henkilö käyttöpaikan tunnistetietojen perusteella. (EU:n Tietosuoja-asetuksen 4 artikla 1 kohta).

Sähköliittymä myydään usein kiinteistökaupan yhteydessä. Tällaisessa tilanteessa sähköliittymää kohdellaan irtaimistona, ja se tulee mainita erikseen kauppakirjassa. Jos sähköliittymää ei ole mainittu erikseen kauppakirjassa, se jää alkuperäiselle omistajalle. (Maanmittauslaitos). Tällöin voidaan verkkopalveluyhtiössä tehdä liittymissopimuksen siirtosopimus, jossa uusi ja vanha omistaja sopivat sähköliittymän siirrosta. Ostetun sähköliittymän tiedot tulevat uuden omistajan henkilötiedoiksi, koska niistä voidaan jälleen tunnistaa välillisesti asiakas. Asiakkaan tilatessa uuden liittymän antaa hän verkkopalveluyhtiölle liittymän tiedot,

joita ovat kartta liittymän sijainnista ja asemapiirros, josta selviää myös tontin rekisterinumero. Liittymäsopimuksen tekemisen yhteydessä sovitaan liittymän suuruudesta. (Enontekiön Sähkö Oy 2019.)

3 ASIAKASTIETOJEN PÄIVITTÄMINEN

3.1 EnerimCIS-asiakastietojärjestelmän käyttöönotto

Tarve asiakastietojen päivittämiselle ja koko asiakasdatan läpi käymiselle lähti liikkeelle uuden asiakastietojärjestelmän käyttöönoton vuoksi. Enontekiön Sähkö Oy:ssä otetaan käyttöön keväällä 2021 uusi asiakastietojärjestelmä EnerimCIS. Pilvipalvelupohjainen ohjelma on tehty vastaamaan energia-alan tarpeita. EnerimCIS mukautuu helposti asiakkaan tarpeisiin. Lisäksi ohjelmaan saa tarvittaessa rajapintoja kolmansien osapuolien käytettäväksi. (Enerim Oy). Enontekiön Sähkö Oy:llä on yksi rajapinta perintätoimiston kanssa. Perintätoimisto on kolmas osapuoli, jolle Enontekiön Sähkö Oy luovuttaa asiakastietojaan. Kolmannella osapuolella tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja (EU:n Tietosuoja-asetus 4 artikla 9 kohta).

EnerimCIS asiakastietojärjestelmän tietoturva on erityisen hyvä, koska sen käyttö on mahdollista ainoastaan palveluntuottajan toimesta tilaamilla IP-osoitteilla. Tietosuojalautakunta on todennut, että IP-osoitettakin pidetään henkilötietona (Tietosuojalautakunta 2006). Lyhenne IP tulee englannin kielen sanoista Internet Protocol. Suomen kielessä kuullaan usein puhuttavan verkko-osoitteesta tai IP-osoitteesta. Numerosarja, joka koostuu neljästä 1-3 numeroisesta luvusta, yksilöi palvelimet ja työasemat. (Jyväskylän yliopisto 2009.)

Asiakastietojärjestelmän koulutukset henkilökunnalle aloitettiin joulukuussa 2020. EnerimCIS-asiakastietojärjestelmä otetaan käyttöön yhtäaikaisesti suuressa osassa Pohjois-Suomen verkkopalveluyhtiöistä. Haastateltaessa henkilötietojen käsittelijöitä, jotka osallistuivat koulutuksiin, ilmeni tietoturvan olleen hyvin hoidettu koulutusten aikana: ”En kyllä koe, että missään vaiheessa olisi tullut sellainen olo, että tässä olisi mitään riskiä”, eräs haastateltavista totesi. Koulutusten jälkeen alkoi Pohjois-Suomen Energiatieto Oy:n, (jäljempänä PSET Oy) vetämät tietojen migraatiot ja migraatioissa havaittujen ongelmien läpikäynti. Ongelmia oli lähinnä datan yhteensopivuudessa ja vanhentuneiden tietojen poistamisessa.

3.2 Datahub – keskitetyn tiedonvaihdon kanava

Toinen iso projekti, jota varten henkilötietoja päivitettiin ja asiakasdataa tarkastettiin on Fingridin Datahub – keskitetyn tiedonvaihdon kanavan käyttöönotto. Datahub on uusi tapa välittää energia-alan tietoja eli sanomia. Sanomissa kulkee tietoa sähkönkäyttöpaikoista ja asiakkaista, tämä tieto tulee Datahubin myötä olemaan ensimmäistä kertaa samassa paikassa ja samassa muodossa. Aikaisemmin tiedonvaihto on ollut useassa eri kanavassa, mutta uuden järjestelmän myötä tiedonvaihto selkeytyy ja nopeutuu koko energia-alalla. (Fingrid.)

Energia-ala on niin sanotusti myyjävetoinen, toisinsanoen kun asiakas sopii energianmyyntisopimuksen, tekee energian myyntiyhtiö asiakkaalle samalla myös verkkopalvelusopimuksen paikallisen verkkopalveluyhtiön kanssa. Sopimukseen tarvittavat tiedot energianmyyjä lähettää sanomana verkkopalveluyhtiölle. Datahubin tarkoitus on mullistaa koko Suomen energia-ala, koska uusien energianmyyjien on aikaisempaa helpompaa tulla mukaan markkinoille, ja näin myös asiakaskokemus paranee kevyemmän organisaation myötä (Sikanen 2016).

Datahubin käyttöönotto vaatii kaikkien energia-alan yhtiöiden datan yhdenmukaistamisen. Esimerkiksi kaikki osoitetiedot tulee jatkossa olla täysin samalla lailla kirjattu. Tiedonvaihtoa varten asiakas-, käyttöpaikka-, tuote- ja sopimustietoja yhdenmukaistetaan, jotta kaikki sanomaliikenteen data olisi täysin samanlaista, ehyttä ja ajantasaista. Tämän takia myös Enontekiön Sähkö Oy:ssä tietoja yhdenmukaistetaan, päivitetään sekä täydennetään. Datahubissa olevan datan tulee olla täysin virheetöntä, joten vaatimukset tiedon laadulle ovat korkeat. Datahub otetaan tuotantoon vuonna 2022.

3.3 Henkilötietojen päivittämisen prosessi

Datahub- ja asiakastietojärjestelmä EnerimCIS-projekteja varten Enontekiön Sähkö Oy:ssä jouduttiin tarkastelemaan asiakas-, käyttöpaikka-, tuote- ja sopimustietoja sekä muokkaamaan ja täydentämään niitä projektien vaatimalla ta-

valla. Tässä opinnäytetyössä keskitytään käsittelemään ainoastaan henkilötietojen päivittämistä, koska jos mukaan otettaisiin myös sopimus- ja tuotetiedot, tulisi aihealueesta liian laaja.

Enontekiön Sähkö Oy:ssä puutteet henkilötiedoissa kohdistuivat lähinnä asiakkaiden henkilötunnusten puuttumiseen. Henkilötunnus puuttui lähinnä norjalaisilta ja ruotsalaisilta asiakkailta. Ulkomaalaisten asiakkaiden kohdalla sovelletaan rekisterinpitäjän kotipaikkaa eli Suomen lainsäädäntöä (Tietosuojalaki 5.12.2018/1050 3§). Tietojen päivittämiseksi ulkomaalaisille asiakkaille lähetettiin tiedote, jossa heitä pyydettiin ottamaan yhteyttä Enontekiön Sähkö Oy:n asiakaspalveluun. Toisena vaihtoestona asiakkaille annettiin mahdollisuus päivittää henkilötietonsa Online-palveluun. Online-palveluun asiakas rekisteröityy omalla asiakas-, käyttöpaikka- ja sopimustunnuksellaan. Palvelussa asiakas näkee asiakkuuteensa ja käyttöpaikkaansa liittyviä tietoja, kuten laskut ja käytetyn energiamäärän käyttöpaikaltaan tunneittain. Samalla saimme mainostettua asiakkaille Online-palvelua, jotta se tulisi laajemmin asiakkaille tutuksi ja jotta he alkaisivat hyödyntämään sitä asioinnissaan. Jos asiakas oli yhteydessä asiakaspalveluun puhelimitse, käytiin puhelun aikana läpi kaikki järjestelmään tallennetut henkilötiedot. Läpikäymisellä haluttiin varmistua, että kaikki yhteystiedot olisivat ajantasaisia ja että puuttuvat tiedot täydennettiin.

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan epätarkat ja aiheettomat tiedot (EU:n Tietosuoja-asetus 16 artikla). Mutta rekisterinpitäjällä on oikeus myös saada ja vaatia rekisteröidystä ajantasaiset tiedot. Rekisteröity, jolla on voimassa oleva verkkopalvelusopimus, on velvollinen ilmoittamaan sopimukseen vaikuttavista muutoksista, jotka koskevat rekisteröityä tai sähkönkäyttöpaikkaa. (Verkkopalveluehdot VPE 2019 2.11). Rekisteröidyllä on siis myös velvollisuus ilmoittaa tietojen muutoksesta rekisterinpitäjälle, mutta valitettavan harvoin tämä seikka muistetaan.

Henkilötiedot korjataan olemassa olevaan asiakastietojärjestelmään Datahubin vaatimalla henkilötiedon ilmoitustavalla. Migraatiossa tiedot viedään uuteen asiakastietojärjestelmään ja Datahubiin. Henkilötietoja korjattiin muiltakin osin kuin

vain puuttuvien henkilötunnusten osalta. Puhelinnumerot, posti- ja laskutusosoitteet sekä sähköpostiosoitteet tulivat olla oikeassa muodossa. Väärässä muodossa olevat henkilötiedot tulivat esiin järjestelmästä erilaisilla poiminnoilla. Väärämuotoiset tiedot korjattiin oikeaan muotoon ilman, että asiakkaaseen oltiin yhteydessä.

3.4 Henkilötietojen käsittelijän kokemus

Teemahaastattelussa henkilötietojen käsittelijät kertoivat, minkälainen prosessi tietojen päivittäminen oli heidän mielestään ja kuinka he omalla toiminnallaan pystyvät minimoimaan tietosuoja- ja tietoturvariskejä. Teemahaastattelu toteutettiin keskustelunomaisesti, jossa kysymykset olivat vain johdattamassa keskustelua sujuvasti seuraavaan kysymykseen. Haastateltavat esiintyivät tässä anonyymeinä.

Datahubia ja EnerimCIS projekteja varten verkkopalveluyhtiössä täytyi tarkastella henkilötietoja, datan yhteensopivuutta ja tietojen oikeudellisuutta. Datassa paljastui puutteita varsinkin henkilötunnusten osalta. Haastattelussa nousi esille, että henkilötietojen käsittelijän näkökulmasta, henkilötunnusten tiedustelu asiakkaalta vaati paljon tiedon antamista ja tilanteen taustoittamista asiakkaalle. ”Nykypäivänä asiakkaat ovat hyvin tietoisia siitä, ettei omaa henkilötunnustaan saa antaa kaiken maailman kyselijöille”, eräs vastaaja selosti.

Asiakkaille, joilta henkilötunnus puuttui, lähetettiin kirje, jossa asiakasta pyydettiin olemaan yhteydessä asiakaspalveluun asiakastietojen täydentämisen vuoksi. ”Tällä lailla saimme asiakkaan luottamuksen. Näin saimme asiakkaat ottamaan meihin yhteyttä, ja heillä tuli luottavaisempi olo antaa henkilötunnus silloin, kun he itse soittivat asiakaspalveluun”, näin eräs haastateltavista totesi. Kysyttäessä, oliko asiakas vastahakoinen antamaan henkilötunnusta, vastaus oli, että muutama asiakas ei olisi halunnut antaa henkilötunnustaan ja väitti, että vain poliisilla on oikeus kysyä sitä: ”Näille asiakkaille täytyi selvittää meidän oikeudet tunnistetiedon käyttämiseen. Sen jälkeen asiakas antoi henkilötunnuksensa, mutta paljon asian taustoittamista se vaati”.

Asiakastietoja päivitettäessä henkilötietojen käsittelijöillä oli erilaisia tyylejä syöttää tiedot asiakastietojärjestelmään: ”Syötän tiedon heti suoraan järjestelmään, jotta se on siellä turvassa palomuurien ja muiden takana, eikä tieto pyöri minun työpöydällä”. Osalla taas tiedot menivät muistilapun kautta asiakastietojärjestelmään. ”Minulle on tuotu lukollinen laatikko, johon saan laittaa lappuni talteen. Se on ollut todella kätevä, jotta saan sitten rauhassa hyvällä ajalla laittaa tiedot järjestelmään”. --”Lukollinen laatikko on turvallinen, koska esimerkiksi illalla täällä käy siivoja ja pöytä tulee olla siisti tietoturvankin takia”.

Haastattelussa kysyttiin asiakkaan tietoisuutta omista oikeuksistaan, ja haastateltavien mukaan asiakkaat eivät tunne omia oikeuksiaan: ”Kukaan ei kysynyt mieltä, että mitä tietoja teillä on minusta”. Tietopyyntöjen määrää kysyttäessä haastateltavat sanoivat, etteivät ole vielä kertaakaan saaneet tietopyyntöä. Kysyttäessä henkilötietojen käsittelyä ulkomaalaisten asiakkaiden kanssa vastaus oli, että silloin käytetään toisen asiakaspalvelijan kielitaitoa, jos oma ei riitä: ”Toinen voi osata hoitaa tilanteen paremmin, jos hänellä on esimerkiksi vahvempi englannin kielen taito, silloin pyydän toista asiakaspalvelijaa apuun”.

Riskien minimoimiseksi tietosuojan ja tietoturvan osalta henkilötietojen käsittelijöillä oli hyviä käytännön esimerkkejä: ”Kun asiakkaita tulee toimistoon, suljetaan ovi, jotta saadaan työ ja keskustelurauha. Seuraava asiakas odottaa käytävällä vuoroaan tai menee toisen asiakaspalvelijan luo”. --”Fyysisen asiakaspalvelun tietoturvaa on parannettu tietokoneen näytön tietosuojakalvolla ja kalusteiden asettelulla. Kalusteita on siirretty siten, että ne itsessään rajaavat asiakaspalvelijalle tilan, ettei asiakas tulisi viereen ja näkisi tietokoneen näyttöä tai pöydällä olevia papereita”.

Työpöydän siisteyttä riskien minimoimiseksi painottivat kaikki haastatteluun osallistuneet: ”Siinä ei pienennetä ainoastaan tietosuojariskiä vaan myös riskiä sille, että jokin paperi katoaisi ja koko asia jäisi näin hoitamatta”. Työpöydän siisteys tulee esille varsinkin silloin, kun on kyse fyysisestä asiakaspalvelusta: ”Joskus asiakkaalle täytyy näyttää tietokoneen näytöltä jotain asiaa ja näytön täytyy kääntää asiakkaalle päin. Silloin työpöydällä ei voi näkyä ylimääräisiä papereita”.

Haastateltavat henkilötietojen käsittelijät toivat keskustelun aikana esille sen, että tietosuoja-asioita täytyy ajatella myös omalla vapaa-ajalla: ”Monesti ihmiset tulevat esimerkiksi kaupassa kysymään, että kuka on ostanut sen talon tai, että kuka muutti tuohon taloon”. --”Varsinkin vanhemmat ihmiset tekevät tätä, kun eivät huomaa, että meitä sitoo salassapitovelvollisuus”. Asiakaspalvelijoista tuntui siltä, että työ henkilöityy liikaakin ja että vapaa-ajalla oltaessa ollaan edelleen verkkopalveluyhtiön asiakaspalvelijoita.

Haastateltavat ovat saaneet tietosuojakoulutuksen, jossa on käyty läpi EU:n tietosuoja-asetus silloin, kun asetus astui voimaan. Heidän mielestään heidän tietotaitonsa tietosuojasta on riittävällä tasolla: ”Muistaa vain pitää aina tiedot minimissä. Täytyy myös pyytää jokaiselta, joka ei ole sopimusosapuoli valtakirjaa asioiden hoitamiseksi. Mielessä tulee pitää myös se, että sähkönmyyjien, sosiaalitoimistojen ynnä muiden senkaltaisten kohdalla täytyy varmistua ensin heidän oikeuksistaan pyytää tietoja asiakkuudesta ja mahdollisesti vielä valtakirjatkin”.

4 REKISTERINPITÄJÄ JA HENKILÖTIETOJEN KÄSITTELIJÄ

4.1 Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisen kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (EU:n Tietosuoja-asetus 4 artikla 7 kohta). Rekisterinpitäjä määrittelee reksiterin käsittelyn tarkoitukset, keinot ja tekee käsittelyä koskevat päätökset. Rekisterinpitäjää painaa myös vastuu siitä, että käsittely tehdään laillisesti ja rekisteröidyn oikeuksien mukaisesti.

Mahdollista on myös yhteisrekisterin pitäminen, jossa kaksi rekisterinpitäjää yhdessä määrittelee käsittelyn keinot ja tarkoitukset sekä vastuualueet tietosuoja-asetuksen toteuttamiseksi. Keskeiset osat näistä määrittelyistä tulee olla rekisteröidyn saatavilla. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 67.)

Rekisterinpitäjän vastuut on säädetty tietosuoja-asetuksessa artikloissa 5 ja 24-36. Yhtenä suurimpana rekisterinpitäjän vastuuna on tehdä tarvittavat tekniset ja organisatoriset toimenpiteet, jotta tietosuoja- ja tietoturvavaatimukset tietosuoja-asetuksessa täyttyvät. Käsittelyn turvallisuus on nostettu esille useassa artiklassa, ja turvallisuuden rikkoutuessa rekisterinpitäjällä on velvollisuus kertoa siitä valvontaviranomaiselle sekä rekisteröidylle. (EU:n tietosuoja-asetus artiklat 24-36.)

4.2 Omavalvontasuunnitelma

Tietosuojan ja tietoturvan toteutumista organisaatiossa tietosuoja-asetuksen vaatimalla tavalla voidaan seurata omavalvontasuunnitelmalla. Sen avulla voidaan ylläpitää, kehittää ja suunnitella tietojen turvaamista ja riskien hallintaa. Omavalvontasuunnitelman avulla pystytään esimerkiksi huolehtimaan siitä, että tietojärjestelmien käyttö ja ylläpito hoidetaan asiaankuuluvalla tavalla. Jos organisaatiossa on käytössä ohjeita ja muita dokumentteja liittyen tietosuojan ja tietoturvan turvaamiseen, omavalvontasuunnitelma tällöin tarpeellinen, jotta pystytään seuraamaan sitä, että esimerkiksi annettua tietosuojaohjeistusta noudate-

taan päivittäisessä työssä. Suunnitelman käyttöönotossa täytyy määrittää seuraamisajat, roolit, vastuualueet ja niiden vastuuhenkilöt. Vastuuhenkilöt huolehtivat valvonnasta ja omavalvontasuunnitelman päivittämisestä.

Omavalvontasuunnitelman tarkoituksena on yhdenmukaistaa käytäntöjä ja varmistaa, että koko henkilökunta noudattaa niitä. Henkilökunnan ja johdon roolit ja vastuualueet tietojen turvaamisessa selkeytyvät. Seuraaminen helpottuu siten, että omavalvontasuunnitelmasta pystytään tarkistamaan, että jokainen on toiminut ja tehnyt heille määrätyt tehtävät siten, kuin on määrätty. Siksi vastuiden ja roolien jakaminen organisaatiossa nousee keskeiseksi osaksi organisaation tietojen riskienhallinnassa. Omavalvontasuunnitelmalla valvotaan, että jokainen hoitaa oman vastuunsa. Vastuut on hyvä kirjata myös sopimuksiin niin ostopalveluissa kuin talon sisäisissä sopimuksissa. Suunnitelmaan on kirjattava, kuinka toteutumista seurataan ja kuinka seuranta on järjestetty. Organisaation vuosikelloon voidaan merkitä omavalvontasuunnitelman seuranta, jotta seuranta olisi säännönmukaista. Omavalvontasuunnitelma toimii hyvänä dokumenttina tietosuoja-asetuksen osoitusvelvollisuuskohdan toteennäyttämisessä. (Andreasson, Riikonen & Ylipartanen 2019, 100-102.)

4.3 Henkilötietojen käsittelijä

Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (EU:n Tietosuoja-asetus 4 artikla 8 kohta). Enontekiön Sähkö Oy:ssä henkilötietojen käsittelijöitä ovat sen omat työntekijät sekä ulkopuoliset palveluntarjoajat kuten PSET Oy. Ulkopuolinen palveluntarjoaja on henkilötietojen käsittelijä rekisterissä silloin, kun se hoitaa rekisteriä ja tekee henkilötietojen käsittelyä Enontekiön Sähkö Oy:n lukuun (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 68). Tiettyjä liike-elämän osa-alueita joudutaan monesti ulkoistamaan, niin myös Enontekiön Sähkö Oy:ssä. Ulkopuolisten palveluntarjoajien kanssa yhtiö on tehnyt kirjalliset sopimukset, joissa on sovittu tarkasti esimerkiksi tietojen käsittelystä. Enontekiön Sähkö Oy:n rekisterissä olevia tietoja saa käsitellä vain

sellainen taho, jolla on EU:n Tietosuoja-asetuksen mukaiset takeet asiantuntemuksessa, luotettavuudessa ja resursseissa, jotta käsittelyn turvallisuus toteutuu (EU:n Tietosuoja-asetus johdanto 81 kohta).

Esimerkiksi PSET Oy:n kanssa Enontekiön Sähkö Oy on tehnyt palvelusopimuksen, jossa on ehdot ja sovitut käsittelytavat, joilla henkilötietoja käsitellään rekisterinpitäjän lukuun. Sopimuksesta on hyvä löytyä ainakin käsittelyn kohde, kesto, luonne ja tarkoitus, henkilötietojen tyyppi, velvollisuudet, kuten salassapitovelvollisuus. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 294-295.)

4.4 Sähkömarkkinoiden tiedonvaihto

Enontekiön Sähkö Oy:tä verkkopalveluyhtiönä velvoittaa tietosuojalaki (5.12.2018/1050), EU:n tietosuoja-asetus ja Energiaviraston säädökset siitä, kenelle ja miten tietoja luovutetaan. Sähkömarkkinalaissa on säädetty, että sähkömarkkinaosapuolien on käytettävä markkinaprosesseihin liittyvien tietojen hallintaan ja välittämiseen sähkökaupan keskitettyä tiedonvaihtoa. Tulevaisuudessa tuo tiedonvaihtokanava on keskitetty tiedonvaihtokanava Datahub, koska laki velvoittaa sähkömarkkinoita myös koko ajan kehittämään sähkönkaupan tiedonvaihtokanavia. Laissa myös säädetään siitä, että tiedon tietoturvataso on asianmukainen ja että ohjelmien edellytykset tehokkaaseen tiedonvaihtoon turvataan. (Sähkömarkkinalaki 9.8.2013/588, 75 a ja b§.)

Sähkömarkkinoilla tietoa luovutetaan puolin ja toisin jatkuvasti tiedonvaihtokanavissa. Käytännössä se tarkoittaa sitä, että kun asiakas tekee sähkönmyyntisopimuksen sähkönmyyjäyhtiön kanssa, hän tekee samalla sähkönsiirtosopimuksen paikallisen verkkopalveluyhtiön kanssa. Eli tiedonvaihto ja -luovutus tapahtuu sähkönmyyjän toimesta heti verkkopalveluyhtiölle. Verkkopalveluyhtiö taas luovuttaa sähkönmyyntiyhtiölle jatkuvasti tietoa käyttöpaikan mittaus- ja kulutustiedoista. Näillä tiedoilla asiakas on välillisesti tunnistettavissa, joten kyseessä on henkilötieto.

Muitakin kuin vain sopimusosapuolen tietoja luovutetaan ja siirretään sähkökaupan tiedonsiirtokanavissa eli sanomissa. Sanomien kautta kulkee verkkopalveluyhtiön lähettämät sähkönkäyttöpaikan kulutus- ja mittaustiedot, jotka kerätään sähkönkäyttöpaikan mittauslaitteistosta. Tiedot luovutetaan sähkönmyyjälle ja loppukäyttäjälle koneellisesti luettavassa, helposti muokattavassa vakiotiedostomuodossa. (Sähkömarkkinalaki 9.8.2013/588, 75 e§). Näiden luovutettujen mittaus- ja kulutustietojen perusteella sähkönmyyjäyhtiö pystyy laskuttamaan loppukäyttäjältä käytetystä energiasta ja loppukäyttäjä pystyy seuraamaan omaa sähkönkulutustaan.

Haastattelussa asiakastietojen käsittelijät mainitsivat, että sähkönmyyjäyhtiötä voidaan hyödyntää asiakastietojen päivittämisessä tai puutteellisten tietojen keräämisessä. Sähkömarkkinan rakenteen vuoksi sähkönmyyjillä on monesti ajantasainen tieto ja täydellisemmät asiakastiedot kuin verkkoyhtiöillä, koska energiasopimuksia uusitaan kahden vuoden välein niiden määräaikaisuuden takia. Haastattelussa todettiinkin: ”Tiedonvaihto toimii myös toisinpäin, eli monesti myyjäosapuoli kysyy verkkopalveluyhtiöltä asiakastietoja. Toki aina näin päin tapahtuvassa kyselyssä täytyy ensin varmistua siitä, että kyseessä on tosiasiallisesti oikea sähkönmyyjä”.

4.5 Tietojen luovuttaminen

Henkilötietoja voidaan luovuttaa tietosuoja-asetuksen puitteissa, kun rekisterinpitäjänä toimii muu kuin viranomainen. Rekisterinpitäjällä ei ole velvollisuutta luovuttaa henkilötietojaan muille kuin valvovalle viranomaiselle ja rekisteröidylle itselleen. Muutoin rekisterinpitäjä itse määrittelee kenelle se tietoja luovuttaa; tämä kuitenkin tulee ilmetä käsittelytoiminnan selosteessa. Rekisteröidyn informointi on tärkeää, jotta rekisteröity tietää minne hänen tietojaan luovutetaan ennen kuin hän antaa tiedot rekisterinpitäjälle. (Haapalehto & Krakau 2020, 207.)

Tietoja ei pääsääntöisesti siirretä Euroopan Unionin tai Euroopan talousalueen (ETA) ulkopuolelle. Euroopan talousalueeseen kuuluvat EU-maiden lisäksi Islanti, Liechtenstein ja Norja. Eurona Unionin ja Euroopan talousalueen ulkopuo-

lelle siirrettäessä henkilötietojen suojan taso heikkenee, ja sen takia EU:n tietosuoja-asetuksessa määritellään siirrolle edellytyksiä, joilla henkilötietoja voitaisiin siirtää kolmasiin maihin tai kansainvälisille järjestöille. (Tietosuojavaltuutetun toimisto 2021). Enontekiön Sähkö Oy:llä ei ole tarvetta siirtää henkilötietoja ETA:n ulkopuolelle.

Isännöitsijä tai konsultti voi tiedustella kiinteistön kulutustietoja. Tietoja ei tule antaa ilman sopimusosapuolen antamaa valtakirjaa. Erikoisissa konsultin tekemissä pyynnöissä kannattaa olla yhteydessä suoraan asiakkaaseen, jolta voidaan puhelimitse kysyä vielä valtakirjan lisäksi tietoja pyynnöstä ja varmistua asiakkaan antamasta toimeksiannosta konsultille. Tietoja voidaan antaa tutkimustyöhön sillä ehdolla, että tietoja ei pystytä kohdentamaan mihinkään tiettyyn käyttöpaikkaan tai asiakkaaseen. Viranomaisille tietojen luovuttaminen perustuu lakiin. Luovutukselle tulee aina olla jokin peruste ja tietopyyntö tulee varmistaa viranomaiselta. Varmistuksessa tulee kysyä, mihin pykälään tiedonantovelvollisuus perustuu ja mitä tietoja viranomainen tarvitsee. Verkkopalveluyhtiö pyytää viranomaisen tietopyynnön aina kirjallisena. (Energiateollisuus 2020.)

Henkilötietoja voidaan luovuttaa eteenpäin verkkopalveluyhtiön asiakkaan edunvalvojalle, joka on holhousviranomaisen tai käräjäoikeuden määräämä (Laki holhoustoimesta 1.4.1999/442). Edunvalvoja edustaa asiakasta sellaisissa asioissa, joita hän ei pysty itse hoitamaan sairauden tai muun painavan syyn vuoksi. Edunvalvojalle voidaan antaa tietoja edunvalvotun asiakkuudesta verkkopalveluyhtiössä sekä antaa tietoja kerätyistä henkilötiedoista. Ennen tietojen luovuttamista on kuitenkin varmistuttava siitä, että asiakas on tosiaan edunvalvottu ja, että edunvalvoja tosiasiallisesti hoitaa henkilön edunvalvontaa. Tällöin edunvalvoja esittää edunvalvontavaltuutuksensa verkkopalveluyhtiölle. (Haapalehto & Krakau 2020, 222.)

Kun henkilö on menehtynyt, hänen elinaikanansa tekemät sopimukset sitovat kuolinpesää. Näin käy myös verkkopalveluyhtiön kanssa tehdyille sopimuksille, sillä ne siirtyvät kuolinpesän nimiin. Kuolinpesän edustajan tulee myös esittää kuolinpesän hoitamisesta valtakirja, jonka hän on saanut muilta kuolinpesän osakkailta. (Finanssivalvonta 2018.)

Kuolleita henkilöitä tietosuoja-asetus ei koske, ja kuolleiden henkilöiden osalta käsittelyä selostetaan useassa eri laissa, kuten esimerkiksi potilaslaissa. (Haapalehto & Krakau 2020, 223). Kun kuolinpesä on jaettu, tulee kiinteistön ja sitä myöten myös sähköliittymän uusi omistaja toimittaa perunkirjoitus verkkopalveluyhtiölle. Sähköliittymä siirretään sitten liittymäsopimuksen siirtosopimuksella uudelle omistajalle.

Haastatteluissa nousi esille, että kuolinpesienkin henkilötunnuksia puuttui asiakastietojärjestelmästä: ”Jonkin verran kuolinpesille saatiin henkilötunnuksia, ja mikä parasta muutama kuolinpesä saatiin kokonaan pois ja sopimukset siirrettyä kuolinpesän osakkaalle. Kun asiakkaalta vaadittiin sähköliittymän siirrossa perunkirjoitusta, lainhuudatusta tai kauppakirjaa tuli asiakkaalta monesti kieltäytymisiä. Näissä tilanteissa asiakasta ohjeistetaan esimerkiksi peittämään summat, koska ne eivät ole oleellisia tietoja sähköliittymän siirrossa uudelle omistajalle”.

Muita tahoja, joille henkilötietoja luovutetaan, ovat kunnan sosiaalitoimistot. Sosiaalitoimistolla on asiakkaalta saatu valtuutus, jonka luvalla sosiaalitoimisto voi hoitaa asiakkaan rahavaroja ja asioita. Asiakkaita autetaan ja opastetaan raha-asioiden hoitamisessa, oli hän toimivaltainen tai ei, mikäli valtuus oli saatu. Ilman valtuuttakin sosiaalitoimistolla on Kuntaliiton (2000) mukaan lain antama oikeus tietyissä tilanteissa hoitaa asiakkaan raha-asioita. Näitä lakeja ovat muun muassa kansaneläkelaki, työeläkelaki, lastensuojelulaki ja laki sosiaalihuollon asiakasmaksuista.

Enontekiön Sähkö Oy antaa Enontekiön kunnan sosiaalitoimistolle tietoja asiakkaan allekirjoittamaa valtuutusta vastaan. Sosiaalitoimisto voi esimerkiksi kysyä asiakkaan velkatilannetta, pyytää maksuaikaa velkaan tai muuttaa esimerkiksi asiakkaan laskutusosoitetta. Yleensä sosiaalitoimen tietopyynnöt koskevat asiakkaan laskuja, jolloin pyydetyt laskut annetaan suoraan sosiaalityöntekijälle. Sosiaalitoimen henkilökunnalle ei anneta mitään asiakastietoja ilman valtuutusta, joka sosiaalitoimen tulee esittää aina tietoja pyydettäessä. Kerran esitetty valtuutus ei riitä, vaan se tulee esittää jokaisen tietopyynnön yhteydessä. (Kuntaliitto 2000.)

Vuokranantajallekin voidaan luovuttaa tietoja, kun kyseessä on rakennuksen tai sen osan suojeleminen sähkönsiirron, -jakelun tai -toimituksen keskeytyessä. Tietoja saa luovuttaa tällaisessa tilanteessa vahingon estämiseksi tai selvittämiseksi. Osapuolen tulee olla kiinteistön omistaja, haltija tai sähkönliittymäsopimuksen osapuoli. (Sähkömarkkinalaki 9.8.2013/588, 75 f §.)

4.6 Käsittelyn läpinäkyvyys ja osoitusvelvollisuus

Henkilötietojen käsittelystä ja tarkoituksesta on ilmoitettava rekisteröidylle, jotta läpinäkyvyyden periaate toteutuu. EU:n tietosuoja-asetuksessa on säädetty läpinäkyvyydestä ja sitä koskevista yksityiskohtaisista säännöistä. Läpinäkyvyyden periaatteella halutaan välttää tilanne, jossa henkilötietojen käsittelyn seuraukset saattaisivat nousta esille vasta silloin kun rekisteröidylle on tapahtunut jo vahinkoa. Rekisteröidyn näkökulmasta henkilötietojen käsittely on epätasapainossa, koska hän ei tiedä, mitä tietoja heistä on kerätty ja mihin kerättyä tietoa käytetään. (Korpisaari, Pitkänen & Warma-Lehtinen 2018.)

Euroopan unionin tietosuoja-asetuksen viidennen artiklan mukaisesti henkilötietoja on käsiteltävä lain- ja asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. Periaatteet ovat tällöin ”lainmukaisuus, kohtuullisuus ja läpinäkyvyys”. Henkilötietoja on kerättävä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Henkilötietoja ei saa käsitellä näiden tarkoitusten vastaisesti tai yhteensopimattomalla tavalla. Kerättyjen henkilötietojen tulee olla asianmukaisia, ja tietojen määrää tulee minimoida eli asiakkaista kerätään ainoastaan välttämättömät tiedot asiakkuuden hoitamiseksi. Henkilötietojen tulee olla täsmällisiä ja niitä tulee päivittää tarvittaessa. Päivitystä, virheellisten tietojen oikaisua ja poistamista yhtiössä onkin tehty käynnissä olevien projektien ansiosta. Tietoja käsitellään siten, että niiden käsittely ei vaaranna tietojen eheyttä ja luottamuksellisuutta. (EU:n tietosuoja-asetus 13 artikla 1 kohta.)

Läpinäkyvyyden periaatteen mukaisesti rekisteröidylle tulee pyydettäessä lähettää tietosuojaraportti. Raportissa imenee kaikki ne tiedot, joita rekisteröidystä on

tallennettu rekisteriin. Enontekiön Sähkö Oy:n uudessa asiakastietojärjestelmässä on mahdollisuus saada suoraan ohjelmasta tietosuojaraportti, jonka voi lähettää rekisteröidylle. Tiedot tulee antaa ymmärrettävällä ja selvällä tavalla, eikä tietojen antamisesta saa periä maksua. Kuitenkin jos rekisteröity esimerkiksi pyytäisi tietojaan tiuhaan, häneltä voitaisiin periä kohtuullinen maksu. Pyynnöstä voidaan myös kieltäytyä, mutta siihen olisi oltava painavat perusteet tai pyynnön olisi oltava kohtuuton. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 178-180). Enontekiön Sähkö Oy ei tee asiakkaistaan profilointia. Jos profilointia kuitenkin harjoitettaisiin, siitä tulisi ilmoittaa rekisteröidylle (EU:n tietosuoja-asetus 5 artikla 1 kohta.)

Osoitusvelvollisuus velvoittaa rekisterinpitäjää varmistamaan, että kaikki mahdollinen on tehty henkilötietojen suojaamiseksi organisaatiossa. Suojaamistoimenpiteet dokumentoidaan, ja suojaamisen laajuus sekä yksityiskohtaisuus riippuu rekisteröityjen tietojen luonteesta, tarkoituksesta, riskeistä sekä rekisterinpitäjän koosta. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 96-97). Osoitusvelvollisuus tarkoittaa myös sitä, että huomioidaan tietosuoja- ja tietoturvariskit. Riskien minimoimiseksi ja tunnistamiseksi rekisterinpitäjän tulee tehdä tarvittavat tekniset ja organisatoriset toimenpiteet.

Osoitusvelvollisuus on yleisvelvoitteena artiklassa 24, jossa rekisterinpitäjää velvoitetaan tekemään asianmukaiset tietosuojaa koskevat toimenpiteet. Käytännössä osoitusvelvollisuutta voidaan todentaa seuraavilla rekisterinpitäjän toimilla:

- Sopimukset
- Henkilökunnan koulutukset ja ohjeistus henkilötietojen käsittelyyn
- Sisäiset ja ulkoiset auditoinnit
- Lokitus ja käyttöoikeuksien rajaaminen
- Seuranta, esimerkiksi omavalvontasuunnitelma ja raportointi, esimerkiksi tietotilinpäätös.
- Tiedon elinkaaren hallinta
- Rekisteröityjen informointi, tietosuojaseloste
- Käsittelytoimien kartoitukset ja inventaariot

- Tietosuojapolitiikka (Andreasson, Riikonen & Ylipartanen 2019, 190.)

4.7 Tietosuojaseloste

Euroopan Unionin tietosuoja-asetus ei edellytä rekisteri- tai tietosuojaselosteen laatimista. Asetuksessa vaaditaan informoimaan rekisteröityä henkilötietojen käsittelystä. Asetuksessa ei myöskään säädetä, missä muodossa informoiminen tulisi tehdä. Tiedot rekisteröidylle henkilötietojen käsittelystä voidaan antaa sähköpostilla, yhtiön internetsivuilla tai kirjeitse. (Voigt & von dem Bussche 2017, 143.)

Asetuksen viidennessä artiklassa on kuitenkin vaatimuksia tiedon laadulle: sen tulee olla ymmärrettävää ja sen on oltava helposti saatavilla. Saatavuuden helppous tarkoittaa sitä, että tietoa ei tarvitse etsiä vaan, että tiedon tulisi olla välittömästi ja selvästi saatavilla. Yhtiöiden kotisivuilla internetissä rekisteröityä on helppo informoida samassa tilanteessa, jossa hänen henkilötietojaan kerättään. Monesti tietosuojaseloste onkin yhtiöiden kotisivuilla kaikkien nähtävillä. Informointikanavaa valittaessa on hyvä miettiä, kuinka asiakkaan kanssa on viestitty, ja kuinka tietoja asiakkaalta on kerätty. (Tietosuojatyöryhmä 2017.)

Tietosuojatyöryhmä on antanut tietosuoja-asetuksen läpinäkyvyyttä koskevat suuntaviivat. Tietosuojaseloste korvaa vanhan rekisteriselosteen ja niiden sisältö on aikalailla samankaltainen, kuin kumotussa henkilötietolain rekisteriselosteessa. Tietosuojaselosteessa tulee ilmetä: rekisterinpitäjän nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, henkilötietojen vastaanottajat tai vastaanottajaryhmät, tietojen säilytysajat, tieto oikeudesta rekisteröidyn oikeuksista, tieto mahdollisesta muusta reksiterin käyttötarkoituksesta sekä maininta tietojen mahdollisesta luovuttamisesta ja siirtämisestä EU- tai ETA-maihin sekä kuvaus rekisterin suojauksesta. (Tietosuojatyöryhmä 2017.)

Enontekiön Sähkö Oy:ssä tietosuojaseloste voitaisiin vastaisuudessa antaa tietosuojaseloste asiakkaalle esimerkiksi sopimusasiakirjojen yhteydessä, joko paperisina tai linkkinä internetsivuille. Osana opinnäytetyön prosessia päivitettiin Enontekiön Sähkö Oy:n tietosuojaseloste (Liite 2.).

4.8 Seloste käsittelytoimista

Tietosuojaselosteesta hieman poikkeava käsittelytoimen seloste on organisaation sisäinen asiakirja, jota ei tarvitse antaa rekisteröidylle. Selosteen tarkoitus on vahvistaa artiklan viisi määräämää osoitusvelvollisuutta. Rekisterinpitäjän pitäjän ja käsittelijän täytyy tehdä omat selosteensa. Sisällöllisesti nämä kaksi poikkeavat jonkin verran, esimerkiksi siten, että käsittelijän tekemä seloste on suppeampi. Koska Enontekiön Sähkö Oy:n suorittama henkilötietojen käsittely ei ole satunnaista selosteen käsittelytoimista tulee olla saatavilla, jos valvontaviranomainen tiedustelee selostetta. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 299-301).

Enontekiön Sähkö Oy:tä käsittelytoiminnan seloste on sama kuin tietosuojaseloste, koska niiden sisältö on pääsääntöisesti sama. Tietosuojaselostetta on laajennettu vastaamaan käsittelytoiminnan selosteen vaatimuksia. Rekisteröityjen informaatioita vaativat artiklat 12-14 ja organisaation sisäiseen osoitusvelvollisuuteen viittaa artikla 30. (EU:n tietosuoja-asetus). Näiden artikloiden vaatimat tiedot löytyvät päivitetystä tietosuojaselosteesta. (Liite 2.).

5 REKISTERÖIDYN OIKEUDET

5.1 Oikeudet tietosuoja-asetuksessa

Verkkopalveluyhtiössä käsitellään luonnollisten henkilöiden henkilötietoja, joilla voidaan suoraan tai välillisesti tunnistaa henkilö, yritys, yhdisty tai jokin muu oikeushenkilö. (Helsingin yliopisto). Rekisteröidyllä on oikeuksia, joita tietosuoja-asetuksessa on käsitelty artikloissa 12-22. Enontekiön Sähkö Oy:ssä uudessa asiakastietojärjestelmässä on yhden rekisteröidyn oikeuden toteuttamiseksi tehty valmis tietosuojaraportti. Rekisteröidyllä on oikeus saada tietää, mitä tietoja hänestä rekisterinpitäjällä on. Asiakastietojärjestelmästä saatava tietosuojaraportti voidaan lähettää asiakkaalle turvasähköpostilla tai kirjeitse, kun asiakas sitä pyytää. (EU:n tietosuoja-asetus 12 artikla.)

Asiakaspalvelussa henkilötietojen käsittelijän tulee tuntea rekisteröidyn oikeudet, jos rekisteröity haluaa käyttää oikeuksiaan. Yleisin rekisteröidyn harjoittama oikeus on oikeus tietojen oikaisemiseen, artiklan 16 mukaisesti. Asiakaspalveluun tietojen oikaisuja tulee rekisteröidyn taholta useita kertoja viikossa. Yleensä oikaisuvaatimukset koskevat laskutusositteen muutosta. Päivitämme tietoja mielellämme, koska siitä on ainoastaan etua yhtiölle, että asiakastiedot ovat ajantasaisia. Aina rekisteröity ei kuitenkaan muista harjoittaa tätä tietojen oikaisun oikeuttaan. Jos rekisteröity ei itse muista oikaista tietojaan, ei rekisterinpitäjä pysty millään tietämään asiakkaan tietojen muutoksesta. Vastuu tietojen oikaisusta on aina asiakkaalla.

Artiklan 17 mukaan rekisteröidyllä on ”oikeus tulla unohdetuksi”. Tätä oikeutta asiakas voi harjoittaa heti, kun artiklan a-alakohdan ehdot täyttyvät eli henkilötietoja ei enää tarvita tai niitä ei enää käsitellä verkkopalveluyhtiön tarpeiden täyttämiseen. Henkilötietoja säilytetään Enontekiön Sähkö Oy:ssä kymmenen vuotta verkkopalvelu- tai liittymissopimuksen päättymisen jälkeen, kirjanpitolain (1336/1997) mukaisesti. Sähkömarkkinalain (588/2013 75 c§) mukaisesti tietoja on verkkopalveluyhtiössä säilytettävä vähintään kuusi vuotta. Tämä kuuden vuo-

den säilytysaika koskee tiedonvaihdon palveluita, markkinaprosesseja ja taseselvitystä. Henkilötietoja voidaan säilyttää kauemmin ainoastaan muun oikeusperusteen takia, joka on kirjanpitolaki. (EU:n tietosuoja-asetus artikla 17.)

Jos asiakas vaatii esimerkiksi artiklan 18 mukaisesti tietojen käsittelyn rajoittamista, se on mahdollista rajoittamalla henkilötietojen käsittelijän oikeuksia. Käyttöoikeuksien rajaamiseksi tarvitaan kuitenkin perusteltu syy asiakkaalta. Asiakkaan suojaamiseksi ja läpinäkyvyyden periaatteen mukaisesti nykyisessä ja uudessa asiakastietojärjestelmässä on olemassa lokitietojen tallennus. (EU:n tietosuoja-asetus artiklat 18 ja 22.)

Tietosuojalaissa rekisteröidylle annetaan oikeus saattaa tieto mahdollisesta tietojen käsittelyssä tapahtuneesta lainsäädännön rikkomisesta tietosuojavaltuutetun käsiteltäväksi. Suomessa valvontaviranomaisena toimii oikeusministeriön alaisuudessa toimiva tietosuojavastaavan toimisto. (Tietosuojalaki 5.12.2018/1050 3§ ja 8§.)

Rekisteröidyn oikeudet asiakaspalveluun:

- Oikeus saada tietoa henkilötietojen käsittelystä.
- Tietojen tarkastus-, rajoitus-, oikaisu- ja poisto-oikeus sekä oikeus tulla unohdetuksi.
- Oikeus siirtää tiedot järjestelmästä toiseen.
- Oikeus vastustaa tietojen käsittelyä.
- Oikeus kieltää automaattinen päätöksenteko.

Rekisteröidyllä on oikeus tietää myös seuraavat asiat:

- Mitä henkilötietoja rekisteröidystä on kerätty?
- Mihin tarkoitukseen tiedot kerätään?
- Luovutetaanko tietoja? Jos luovutetaan, niin minne?
- Luovutetaanko tietoja kolmansiin maihin tai kansainvälisille järjestöille?
- Kuinka kauan henkilötietoja säilytetään?
- Miten rekisterinpitäjä on kerännyt henkilötiedot?

- Käyttääkö rekisterinpitäjä automatisoitua päätöksentekoa? Jos käytetään niin kuinka se vaikuttaa rekisteröityyn?
- Oikeus tehdä valitus valvontaviranomaisille. (EU:n tietosuoja-asetus artikla 3. luku.)

5.2 Lokitiedot

Asiakkaiden turvallisuuden ja oikeuksien takaamiseksi jokaisessa ohjelmassa, jossa henkilötietoja käsitellään, on ohjelman sisäinen lokitietojen tallennus. Lokitiedoilla voidaan selvittää, mitä henkilötietoja tarkasteltiin, kuka niitä tarkasteli, milloin tarkastelu tapahtui ja tehtiinkö tarkastelun aikana muutoksia. Lokitiedotkin ovat henkilötietoja, eli lokista muodostuu henkilörekisteri. Tällöin lokitietojen käsittelyssä tulee ottaa huomioon myös Euroopan Unionin tietosuoja-asetukset. Lokitiedoilla turvataan myös henkilötietojen käsittelijän oikeuksia. (Kyberturvallisuuskeskus 2020.)

Mahdollisissa henkilötietojen käsittelijän tekemässä väärinkäyttötapauksissa lokitietojen avulla pystytään paikantamaan, kuka tietoja on katsonut, milloin ja minkä takia. Lokitietojen säilytysaika vaihtelee tietojärjestelmästä, mutta pääsääntöisesti tietojen säilytysaika on 6-24 kuukautta. Lokitietojen kerääminen on osana tietoturvaa, jotta henkilötietojen käsittely olisi turvallista ja tietosuoja-asetuksen mukaisesti läpinäkyvää. Rekisteröidyllä on oikeus tietää, kuka hänen henkilötietojaan on tarkistellut ja minkä takia. Lokien käsittely perustuu lakeihin, joita ovat muun muassa Henkilötietolaki 22.4.1999/523 ja Laki yksityisyyden suojasta työelämässä 13.8.2004/759 ja Tietoyhteiskuntakaari 7.11.2014/917. (Viestintävirasto 2016.)

5.3 Tietojen tarkastuspyyntö

Rekisteröidyllä on oikeus tehdä tarkastuspyyntö henkilötiedoistaan. Asiakkaan täytyy kertoa pyynnössä omat yhteystietonsa ja nimensä, minkälaisia tietoja hän haluaa tarkistella sekä miltä aikaväliltä tarkastettavat tiedot tulee olla ja missä muodossa asiakas haluaa tiedot. Rekisterinpitäjän tulee vastata tarkastuspyyn-

töön kuukauden kuluessa pyynnöstä. Rekisterinpitäjä voi saada lisäaikaa ja toimittaa tiedot kolmen kuukauden kuluessa, mutta tähän tulee olla painava syy. Jos tietoja rekisteröidylle ei anneta tässä ajassa, hänellä on oikeus tehdä tietosuojavaltuutetulle kantelu tietosuojaoikeuksiesi loukkaamisesta. (Tietosuojavaltuutetun toimisto 2021.)

Tietosuoja-asetuksen 15 artiklassa on säädetty oikeudesta päästä käsiksi tietoihin. Rekisteröidylle tulee toimittaa seuraavat tiedot: käsittelyn tarkoitus, henkilötietoryhmä, vastaanottaja tai vastaanottajat myös mahdolliset kolmansien maiden vastaanottajat tai kansainväliset järjestöt, tietojen säilytysaika sekä tieto mahdollisesta profiloinnista. (EU:n tietosuoja-asetus artikla 15.)

6 TIETOSUOJARISKIT

6.1 Tietosuojasta

Jokaisella on oikeus tietosuojaan, sillä se on perusoikeus, jolla turvataan henkilöiden tietoja. Tietosuoja antaa rekisteröidylle tiedon, milloin ja millä edellytyksillä hänen henkilötietojaan käsitellään. (Tietosuojavaltuutetun toimisto 2021). Tietosuoja hyvin toteutettuna on hyödyksi ja suojaksi organisaatiolle, henkilöstölle ja asiakkaille. Sopivasti mitoitettuna tietosuoja parantaa asiakaskokemusta sekä parantaa koko asiakasprosessin sujumista. Lisäksi se luo myös luottamusta asiakassuhteeseen toimialasta riippumatta. Liian tiukka tietosuoja taas tekee taas prosesseista raskaita ja hitaita, tietosuojan taso täytyy mitoittaa ja räätälöidä juuri oman organisaation tarpeiden mukaisesti. Tietosuoja parantaa henkilökunnan oikeusturvaa, lisää organisaation tehokkuutta ja säästää kustannuksia. Tietosuojan toteuttaminen lain mukaisesti on kaikkien velvollisuus ja etuoikeus. Organisaation hyvä tietosuojan taso sekä auttaa henkilökuntaa työssään että saa viihtymään työpaikalla. Tietosuojan historia ulottuu antiikin aikoihin saakka; silloin lääkärit valoivat Hippokrateen valan potilastietojen suojaamiseksi. Tänä päivänäkin tietosuojassa on kyse noista samoista asioista kuin antiikin aikanakin eli luottamuksesta ja osaamisesta. (Andreasson, Riikonen & Ylipartanen 2019, 19-20.)

Tietosuoja on Suomen perustuslaissa säädetty kohdassa yksityiselämän suoja: ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu” ja ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton”. (Suomen perustuslaki 11.6.1999/731, 10§). Toisin sanoen tietosuoja on meidän perusoikeutemme ja jokaisen meistä tulee kunnioittaa tätä niin työelämässä kuin myös omassa yksityiselämässäkin. Yksityisyyden menettäminen on peruuttamatonta ja sen voi menettää vain kerran. Yksityisyytensä menettänyt henkilö menettää henkilökohtaisen luottamuksen, ja sitä on mahdotonta saada takaisin minkäänlaisella rikosoikeudellisella rangaistuksella. (Andreasson, Koivisto & Ylipartanen 2019, 81.)

Tietosuojan riittämättömyys altistaa rekisteröidyn myös identiteettivarkaudelle, jossa uhrin henkilö- ja tunnistautumistietoja tai muuta yksilöivää tietoa käytetään väärin ja haitallisesti. Uhri voi saada oikeudettomasta tietojen käytöstä omaisuus,

maine- tai tietovahinkoa. (Rikoslaki 19.12.1889/39, 38 luku, 9a§). Rikoslaissa luvussa 38 on säädetty kaikista tieto- ja viestintärikoksista, kuten salassapitorikoksesta, viestintäsalaisuuden loukkauksesta ja tietoliikenteen häirinnästä.

6.2 Riskien arviointi

Henkilötietojen käsittelyä on henkilötietojen kerääminen, säilyttäminen, käyttö, luovuttaminen, siirtäminen ja poistaminen. Ennen henkilötietojen käsittelyä on arvioitava riskit, joita käsittelyyn kuuluu, ja on tehtävä toimintasuunnitelma, riskien realisoitumisen varalle. (Tietosuojavastaavan toimisto 2021). Riskien realisoituminen tarkoittaa sitä, että rekisteröity kärsii henkilötietojen käsittelyn aiheuttamasta fyysisestä, aineettomasta tai aineellisesta vahingosta. Vahinko voi aiheuttaa rekisteröidylle sosiaalista tai taloudellista vahinkoa tai rekisteröity voi joutua identiteettivarkauden tai petoksen uhriksi. (Tietosuoja-asetus johdanto 73-76.)

Riskianalyysillä tunnistetaan tarvittavat toimenpiteet, joiden avulla riskien realisoituminen estetään ja henkilötietojen oikeanlainen käsittely turvataan. Riskiarvio on tehtävä aina rekisteröidyn näkökulmasta, koska mahdollisessa henkilötietojen loukkauksessa uhrina on aina rekisteröity. Riskiarviossa on huomioitava henkilötietojen käsittelyn asiayhteys, laajuus, luonne ja tarkoitus. (Tietosuojavaltuutetun toimisto 2021.)

Enontekiön Sähkö Oy:ssä riskienarviointi on tehty Energiaviraston vaatimassa valmiussuunnitelmassa. Lisäksi sähkömarkkinalain (588/2013) 28 pykälässä säädetään myös valmiussuunnitelmasta. Valmiussuunnitelman pääpaino on verkkoon kohdistuvien häiriötilanteiden ja muiden uhkien analysoinnissa ja niihin valmistautumisessa. Valmiussuunnitelmassa on mukana sekä juridiset riskit että tietoihin kohdistuvat uhat, joihin tietosuojakin kuuluu. Valmiussuunnitelmaan on tehty myös vaikutuksenarviointi. Valmiussuunnitelma ei ole julkinen asiakirja. (Enontekiön Sähkö Oy valmiussuunnitelma 2019.)

6.3 Riskienhallintastandardit

Riskien hallintaan on olemassa hyviä työkaluja. Yksi näistä työkaluista on ISO 31000 riskienhallintastandardi ja toinen ISO/IEC 27001 (International Electrotechnical Commission) tietoturvallisuuden standardi. Molemmat standardit on tarkoitettu organisaation kehittämiseen, ja niiden käyttämistä voitaisiin harkita myös Enontekiön Sähkö Oy:n toiminnassa. ISO/IEC 27001 standardin avulla sitoudutaan tietoturvapolitiikkaan, eli suojaamaan organisaation tieto-omaisuutta. (Andreasson, Koivisto & Ylipartanen 2019, 42-43).

Tietosuojaan on saatavilla myös oma SFS-ISO/IEC 29100 standardi, jonka avulla organisaatio voi arvioida hallinta kykyään tietoliikenteen prosesseissa. Standardin avulla tietosuoja-asetus otetaan osaksi kaikkia organisaation toimintoja ja kehitetään tietosuojamalli, joka määrittelee yleisen termistön, henkilötietoja käsittelevät toimijat, roolit ja vaatimukset. (Suomen Standardisoimisliitto SFS ry).

ISO on lyhenne sanoista The International Organization for Standardization, joka tarkoittaa kansainvälistä standardisoimisjärjestöä. ISO 31000 on riskienhallinnan työkalu, jota voivat hyödyntää eri toimialojen, eri kokoiset organisaatiot. Standardi auttaa organisaatiota ottamaan riskienhallinnan osaksi hallintoa, strategiaa, arvoja ja työkulttuuria. Standardin avulla tunnistetaan riskit ja niiden vaikutukset, sekä tehdään riskienhallinnasta keskeinen osa organisaation menestymistä. (Hardy 2015, 135-136.)

7 TIETOTURVARISKIT

7.1 Tietoturvasta

Tietosuojan varmistamiseksi omassa työssään tulee jokaisen huolehtia myös tietoturvasta. Tietosuoja ja tietoturva kulkevat käsi kädessä, toinen toistaan tukien. Tietoturvallisuudella tarkoitetaan tietoliikenteen, palveluiden ja tietojen suojaamista erilaisilla teknisillä ja hallinnollisilla ratkaisuilla. Näillä ratkaisuilla turvataan tiedon eheys ja käytettävyys. Organisaation johdolla on avain asema tietoturvallisuuden toteutumisessa. Johdon tekemät ratkaisut tietoturvallisuuden kehittämisessä ja resurssien tarjoamisessa antavat mahdollisuudet koko henkilökunnalle osallistua tietoturvan parantamiseen. Organisaatiossa tulee asettaa tiedolle tavoiteltava turvallisuustaso, jota pyritään saavuttamaan tietoturva- ja riskienhallintapolitiikalla. Henkilökunnalle laaditaan näiden pohjalta tietoturvaohje, jonka avulla jokainen organisaatioon kuuluva osaa toteuttaa ja turvata organisaation tietoja. (VAHTI 3/2007, 15.)

Tietoturvan tehtävänä on turvata tärkeiden tietoa ylläpitävien järjestelmien ja verkkojen toimiminen kaikissa olosuhteissa. Tietoturvan avulla estetään tietojen tuhoutuminen, vääristyminen ja minimoidaan riskit, mikäli mahdollinen tietoturvaloukkaus tapahtuisi. Tietoturvan täytyy olla osana joka päivistä organisaation toimintaa, ja jokainen organisaation osan tulee omalta osaltaan varmistaa, että tietoturvaa toteutetaan. (Andreasson & Koivisto 2013, 29.)

Tietoturvan uhkana ovat usein henkilöstöstä aiheutuvat uhat, jotka ovat tahallisia ja tahattomia. Tietojen eheys, luottamuksellisuus ja käytettävyys voivat vaarantua, jos henkilökuntaa ei kouluteta ja kehitetä, koska jopa puolet kaikista tietoturvarikkomuksista johtuu organisaation omista menettelytavoista. VAHTI 2/2008 -ohjeessa vahinkojen määrän rajoittamiseksi esitellään neljän kohdan riskienhallintamenetelmä. Menetelmän ensimmäisenä kohtana on riskin välttäminen, ja siinä henkilöstön sijoittelulla ja toimenpiteiden suunnittelulla pyritään vähentämään tapahtuman todennäköisyyttä. Toisena kohtana on riskin estäminen liikkumisen ja toiminnan rajoituksilla. Rajoituksia voivat esimerkiksi olla kulunvalvonta organisaation tiloissa ja ohjelmien käyttöoikeuksien rajoittaminen. Kolmantena

toimenpiteenä on riskin havaitseminen, jolla pyritään estämään tietojen väärinkäyttö ja paljastamaan mahdollinen tietosuojarikkomus. Havainnointia voidaan tehdä lokitietojen ja erilaisten valvontalaitteistojen avulla. Viimeisenä toimenpiteenä on vahingosta toipuminen, eli kuinka menetellään sitten, kun vahinko on jo tapahtunut. (VAHTI 2/2008.)

Tietoturvan riskien hallinnassa on ymmärrettävä, että tietoturvallisuus on organisaation etu, joka voi helposti vaarantua. Tietoturvan suunnittelussa on mietittävä myös käyttöystävällisyyttä. Liiallinen tietoturva tekee tiedon saannin hankalaksi ja kankeasti käytettävää, liian vähäinen taas asettaa tiedon alttiiksi vaaralle. Organisaation on löydettävä tasapaino prosesseissa, jotta tietoturvaa pystytään toteuttamaan tehokkaasti. (Land, Ricks &Ricks 2014, 28.)

Tietoturvaa säätelee myös laki. Keskeisimmät lait ovat Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011), eli niin sanottu tietohallintolaki. Lain tarkoituksena on tehostaa ja parantaa julkisia palveluja sekä niiden saatavuutta. Lailla halutaan parantaa myös tietojärjestelmien yhteensopivuuden edistämistä ja varmistamista.

7.2 Työskenneltäessä huomioitavaa

Etätyö on varmasti tullut jäädäkseen työkulttuuriimme. Tietoturva tulee huomioida myös kotona työskennellessä. Kotona työskenneltäessä on pidettävä huolta siitä, että omat perheenjäsenet eivät käytä työpaikan tietokonetta tai muita älylaitteita. Vaikka esimerkiksi lapset kirjautuisivat toisena käyttäjänä tietokoneelle, he voivat tietämättömyyttään ja vahingossa ladata koneelle muun muassa haittaohjelman. Tällöin kone on altistunut ja tietosuoja on vaarantunut. Kotitoimistolla työskenneltäessä tulee tarkkaan myös arvioida tulostettavien asiakirjojen tarpeellisuus. Kotitoimistolla ei välttämättä ole mahdollisuutta lukita asiakirjoja turvalliseen kaappiin, joten asiakirjojen tulostamisen kannattaa jättää toimistopäiville, jolloin asiakirjan pystyy heti arkistoimaan. (Järvinen & Rousku 2017, 48-51).

Tietoja tallennetaan ainoastaan organisaation hyväksymiin tallennusalustoihin. Tietojen lähettämisessä tulee myös käyttää ainoastaan hyväksyttyjä menetelmiä.

Sähköpostin välityksessä ei saa missään tapauksessa lähettää henkilötunnusta, vaan henkilötunnuksen sisältävän viestin lähetys tapahtuu suojatulla sähköpostilla. Tietosuoja-asetuksen mukaisesti tietoja on käsiteltävä tavalla, joka varmistaa tietojen asianmukaisen turvallisuuden. (Tietosuoja-asetus 5 artikla, alakohta f).

Haastateltaessa henkilötietojen käsittelijöitä ilmeni asiakkaiden tietämättömyys sähköpostin suojattomuudesta: ”Asiakkaat eivät tienneet, ettei sähköpostin välityksellä saa lähettää henkilötunnusta. Neuvoimme asiakasta soittamaan tai lähettämään henkilötunnuksen esimerkiksi tekstiviestillä, jos sitä ei pystynyt sanomaan puhelun aikana. Asiakkaat monesti omalla riskillä kuitenkin lähettävät henkilötunnusta sähköpostitse, jolloin riski on asiakkaan tiedostama ja valitsema”. ”Asiakkaita neuvotaan lähettämään perunkirjoitukset, lahja- ja kauppakirjat aina kirjeitse tai verkkopalveluyhtiö voi lähettää suojatun sähköpostin, johon voi vastata ja liittää dokumentti suojatusti”.

Kokonaisturvallisuuteen tulee myös panostaa, olipa työpiste missä tahansa. Salasanojen ja käyttäjätunnusten tulee olla ainoastaan käyttöoikeuden omaavalla henkilöllä. Salasanoja tarvitaan nykyisin paljon, ja niiden kaikkien muistaminen voi olla hankalaa. Salasanoja voidaan tallentaa niitä varten suunniteltuihin hallintaohjelmiin. Hallintaohjelman tulee olla tietoturvallinen ja ehdottomasti oman organisaation hyväksymä. (Järvinen & Rousku 2017, 57). Automaattikirjautumisia työpaikan laitteilla ei saa olla ollenkaan, koska esimerkiksi laitteen katoamisen tai varastamisen yhteydessä ulkopuolinen henkilö pääsisi suoraan esimerkiksi sähköpostiin ilman salasanan antamaa suojaa. Työpaikan laitteet on myös suojattava salasanalla.

Sähköverkkoasentajat käyttävät Mitello-jakeluverkon kunnossapito-ohjelmaa linjalla työskennellessään älypuhelimen kautta. Jos älypuhelin katoaisi tai varastettaisiin, saisi ulkopuolinen henkilö saisi pääsyn helposti koko verkkopalveluyhtiön asiakastietodataan. Tämän takia laitteiden suojaus on ensiarvoisen tärkeää ja kokonaan työntekijän omalla vastuulla.

Kokonaisturvallisuuteen kuuluu myös oman ympäristönsä tunnistaminen. Ympäristö tulee huomioida esimerkiksi silloin, kun puhutaan puhelimessa. On mietittävä, kuka voi kuulla keskustelun ja minkälaista tietoa keskustelun aikana kerrotaan. Tämä on huomioitava varsinkin työmatkoilla ja kotitoimistolla työskenneltäessä. Internetissä ja sähköpostissa on omat vaaransa kuten, tietojenkalastteluviestit, sähköpostihuijaukset ja virusviestit. Internetsivujen ja sähköpostiviestien turvallisuus tulee arvioida ennen, kuin niitä päätetään avata. (Järvinen & Rousku, 58-100). Tietokoneen näyttö tulee aina olla peitettynä niin sanotulla tietoturvakalvolla. Suositeltavaa on myös, että tietokoneen kamera on peitetty, jotta esimerkiksi mahdollinen haittaohjelma ei pääse hallinnoimaan kameran toimintoja.

Kotoa ja työmatkoilta tehtäessä töitä internettiä selataan ainoastaan VPN-yhteyden kautta. VPN tulee englannin kielen sanoista Virtual Private Network, eli virtuaalinen erillisverkko ja sen tarkoitus on suojata yksityisyytesi internetissä. Yhteyden avulla salataan verkkoliikenne, jotta ulkopuoliset tahot eivät pääsisi kiinni verkkoliikenteeseen. VPN-yhteyden avulla et ole suoraan yhteydessä internettiin, vaan olet VPN-tukiaseman kautta yhteydessä. Näin pystytään piilottamaan oma IP-osoite, jottei käyttäjää pystytä tunnistamaan internetissä. (F-Secure 2021.)

7.3 Kyberturvallisuus

Kyberuhat ovat varteenotettavia vaaroja niin isoille ja kuin pienillekin yrityksille. Yleisimmät kyberuhat pienyrityksille ovat tietojenkalastelu, haittaohjelmat ja kiristyshaittaohjelmat. Kyberuhilta voidaan suojautua tekemällä päivittäisiä suojautumiskeinoja. Yksi turvallisuuden parantamisen keino on pitää tietokoneet ja muut älylaitteet päivitettyinä. Päivitykset tulee tehdä aina, kun uusi päivitys on saatavilla. Koneiden päivittäminen antaa paremman tietoturvan ja suojan sekä parantaa ominaisuuksia ja nopeutta. Varmuuskopioi yrityksen toiminnan kannalta keskeiset tiedot ja säilytä niitä erillään alkuperäisistä. Tietojen varmuuskopioinnilla taataan yrityksen toiminta tietojen menettämisen jälkeenkin sekä täytetään lailliset velvoitteet esimerkiksi kirjanpitolain säilytysaikojen noudattaminen. Suosi monivaiheista tunnistautumista, koska se parantaa turvallisuutta ja hankaloittaa mahdollista hakkerointia. Henkilökuntaa suositellaan käyttämään myös vahvoja

ja aina erilaisia salasanoja kirjauduttaessa työpaikan ohjelmistoihin. (Traficom 2020.)

Käyttöoikeuksien hallinnalla voidaan parantaa myös kyberturvallisuutta. Henkilöstöllä, jolla ei ole tarvetta tietoon, ei tulisi olla myöskään oikeutta päästä käsiksi tietoon. Henkilökuntaa tulee myös kouluttaa ja harjoittaa yleisesti tietoturvallisuusasioissa ja tietoturvapoikkeamien sattuessa kohdalle. Tietoturvapoikkeamista tulee aina ilmoittaa mahdollisimman pian esimiehelle, jotta tietoturvaloukkauksen jälkeinen prosessi voidaan aloittaa. (Traficom 2020). Enontekiön Sähkö Oy:ssä tietoturvaloukkaukseen on varauduttu verkkopalveluyhtiön valmiussuunnitelmassa.

8 HENKILÖTIETOJEN KÄSITTELY

8.1 Huolellisuusvelvoite

Rekisterinpitäjällä sekä rekisterinpitäjän lukuun toimiville toimijoille on sama huolellisuusvelvoite, joka oli henkilötietolain yleisvelvoite. Kumotussa henkilötietolain viidennessä pykälässä asetettiin pitkälti samaa kuin tietosuoja-asetuksen viidennessä artiklassakin. Tietojen käsittelyn tulee olla laillista, huolellista ja sen tulee noudattaa hyvää tietojenkäsittelytapaa. Käsittely ei saa rikkoa rekisteröidyn yksityiselämän suojaa tai muita yksityisyyden suojaa turvaavia perusoikeuksia. Käsittelytapa on yksi huolellisuusvelvoitteen ilmentymä, oli sitten huolellisuusvelvoitteesta säädetty henkilötietolaissa tai EU:n tietosuoja-asetuksessa. (Vanto 2011, 39.)

Kun henkilötietoja käsitellään, tulee käsittelijällä olla koko ajan mielessä häntä koskevat velvoitteet ja vaatimukset. Asiakaspalvelutilanne, joissa henkilötietoja kerätään, on usein hektinen tilanne. Henkilötietojen käsittelijän tulee tehdä tilanteessa monta työvaihetta yhtäaikaisesti. Esimerkiksi asiakkaan kanssa täytyy keskustella asiakkuudesta ja samalla kirjata ylös tietoja asiakastietojärjestelmään. Koko asiakaspalvelutilanteen ajan henkilötietojen käsittelijän on pidettävä huolta tietosuojasta ja tietoturvasta.

8.2 Asiakaspalvelutilanne

Asiakaspalvelutilanteessa asiakas tunnistetaan kysymällä asiakkaalta identifioivia kysymyksiä kuten nimi, henkilötunnus ja sähkön käyttöpaikan osoite. Näiden tietojen perusteella asiakas tunnistetaan ja asiakaspalvelutilannetta voidaan jatkaa eteenpäin. Kuitenkin monesti varsinkin puhelimessa suoritettavan asiakaspalvelun ja tunnistamisen aikana tulee mieleen, että onko puhelimen toisessa päässä oikeasti kyseinen henkilö. Tätä asiaa on pohdittu myös Tietosuojavaltuutetun toimistossa, jossa tietosuojavaltuutettu Anu Talauksen mielestä henkilötunnusta ja nimeä ei tulisi käyttää ihmisen tunnistamiseen. Tunnistautuminen puhelimessa on kuitenkin haasteellista, ja keinot ovat rajallisia. HUSin hallintoylilääkä-

rin mukaan väärinkäyttötapauksia on kuitenkin vähän ja riski on melko pieni. (Näveri 2020). Verkkopalveluyhtiön näkökulmasta myös riski väärinkäyttötapauksiin on pieni, mutta silti varteenotettava mahdollisuus.

Henkilötietojen käsittelijät kertoivat haastattelussa, että eteen voi tulla myös tilanteita, joissa esimerkiksi samassa sähkönkäyttöpaikassa asuva kysyy asuinkumppaninsa nimissä olevasta verkkopalvelusopimuksesta. ”Tällaisissa tilanteissa pyydetään itse sopimuksen osapuolta soittamaan ja keskustelemaan asiasta. Sopimusosapuolen kanssa voidaan sitten asioida ja kertoa hänelle asiakkuuden tietoja. Asiakasta voidaan myös ohjeistaa, että samassa käyttöpaikassa asuva henkilö voitaisiin ottaa mukaan sopimukseen sopimusosapuolena. Tällöin hänellä on samanlaiset oikeudet saada tietoja ja hoitaa asiakkuutta, koska vain sopimusosapuolelle voidaan antaa tietoja asiakkuudesta”.

Aviopuolisolla on oikeus tietää toistensa tekemistä sähkösopimuksesta, kun sopimus koskee heidän yhteistä kotiaan. Jommankumman tekemä sopimus yhteiseen kotiin aiheuttaa velkavastuuta, ja on siten molemmat avioliiton osapuolet ovat siitä vastuussa. (Avioliittolaki 13.6.1929/234 52 §). Alle 18- vuotiaille lapsille tietoja ei luovuteta edes valtakirjalla, koska verkkopalveluyhtiö ei lähtökohtaisesti tee sopimuksia alle 18-vuotialle henkilöille. Alaikäinen ei voi itselleen myöskään tehdä minkäänlaista sopimusta verkkopalveluyhtiön kanssa, koska hän ei voi tehdä luottosopimusta eikä siten saatavia voida periä. (Kuluttajansuojalaki 20.1.1978/38.)

Luottamuksen säilyttäminen asiakassuhteessa on avainasemassa. Se tarkoittaa sitä, ettei tietoja anneta kuin sellaisille henkilöille, jotka ovat oikeutettuja niihin. Tiedot on myös säilytettävä siten, ettei muut pääse niihin käsiksi. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 306). Tietoja täytyy säilyttää siten, ettei ulkopuoliset pääse käsiksi niihin. Tähän kuuluu myös oman työpisteen pitäminen sellaisessa kunnossa, ettei ulkopuolinen henkilö pääse näkemään käsiteltäviä tietoja.

8.3 Vaitiolovelvollisuus

Suomen lainsäädännössä Tietosuojalaki (5.12.2018/1050, 35 §) velvoittaa henkilötietojen käsittelijää vaitiolovelvolliseksi. Toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta tai liikesalaisuuksista ei saa ilmaista sivullisille, tai käyttää tätä tietoa toisen hyödyksi tai vahingoksi. Toisin sanoen henkilötietojen käsittelijä ei saa sanoa esimerkiksi sähkönkäyttöpaikan katkaisusta muille kuin sopimusosapuolille, katkaistun käyttöpaikan sähkönmyyjälle ja verkkopalveluyhtiön henkilökunnalle. Henkilökunnallekin vain niiltä osin, kuin on toimenpiteen toimeenpanon kannalta tarpeellista. Asiakaspalvelutilanteessa voi esimerkiksi tulla eteen tilanne, jossa aikuinen lapsi kysyy vanhempiensa laskunmaksutilannetta tai syytä sähköjen pois kytkemiseen. Kyselyyn tulee vastata kielteisesti, vaikka aikomukset ja periaate omien vanhempien huolenpidosta ovatkin hyviä.

Tietoja voidaan antaa ainoastaan sopimusosapuolen kirjallisella suostumuksella eli valtakirjalla. Valtakirja on kirjallinen viesti siitä, että kolmas osapuoli on oikeutettu tekemään oikeustoimia valtuuttajansa puolesta. Yleisin valtakirjan tarkoitus on valtuuttaa jokin kolmas henkilö hoitamaan valtuuttajan taloudellisia asioita. Valtakirja voidaan antaa myös suullisesti, mutta Enontekiön Sähkö Oy:ssä valtakirja vastaanotetaan aina kirjallisena ja siitä otetaan kopio, jotta asianmukaisuus voidaan myöhemminkin todentaa. (Financer 2020.)

Muita lakeja ja asetuksia, joissa säädetään salassapitovelvollissudesta ovat EU:n tietosuoja-asetus ja Sähkömarkkinalaki. Euroopan unionin tietosuoja-asetuksessa artiklassa 90 on säädetty salassapitovelvollisuudesta. Artiklassa säädetään, että salassapitovelvollisuuden piiriin kuuluvia tietoja tulee luovuttaa valvontaviranomaiselle sen tehtävien suorittamiseksi. (EU:n tietosuoja-asetus artikla 90). Sähkömarkkinalaissa on säädetty salassapitovelvollisuudesta ja hyväksikäyttökiellosta, mutta tämä pykälä käsittelee niistä enemmän maanpuolustuksen ja väestönsuojelun näkökulmasta. (Sähkömarkkinalaki 9.8.2013/588, 76§.)

8.4 Käyttö- ja salassapitositoumus

Työntekijöille tehdään monesti tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus. Sitoumuksessa tulisi olla ainakin seuraavat kohdat:

- Työntekijä käsittelee tietoa huolellisesti ja hyvän hallintotavan mukaisesti.
- Salassapitovelvollisuus: salassa pidettäviä tietoja ei saa välineriippumattomasti vuotaa organisaation ulkopuolelle.
- Vaitiolovelvollisuus, jossa työntekijä sitoutuu kieltoon, jossa tietoja ei ilmaista sivullisille tai käytetä tietoa omaksi tai toisten hyödyksi tai vahingoksi.
- Työntekijä ei saa ottaa tietoja selville kuin omien työtehtäviensä hoitamiseksi. Jos työntekijä rikkoo sitoumusta siitä voi seurata rikos-, työ- ja vahingonkorvaus oikeudellisina seurauksina.
- Sitoumus koskee työntekijää palvelussuhteen ajan ja myös sen jälkeen. Sitoumuksessa on hyvä olla myös mainintoja tietoturvasta.
- Työntekijä vastaa tietokoneista ja älylaitteista siten, että laitteet tai niiden sisältämä tieto ei joudu vääriin käsiin.
- Tietoja luovutetaan ulkopuolille ainoastaan lain tai valtakirjan luvalla.
- Tietoja ei tulosteta tai tallenneta organisaation ulkopuolisille laitteille.
- Sähköisten viestintävälineiden käytössä noudatetaan annettuja ohjeita ja määräyksiä. Sähköisiä viestintävälineitä ovat pikaviestipalvelut, sähköposti, kalenteri ja erilaiset älypuhelimen sovellukset. Jos salassa pidettäviä tietoja täytyy lähettää sähköisenä viestinä, tehdään se ainoastaan käyttämällä suojattua sähköpostia.
- On varmistettava, etteivät sivulliset kuule tai näe työtietoja niin työpaikalla, työmatkalla tai kotitoimistolla. Kotitoimistolla olevia laitteita tai etäyhteysvälineitä ei saa antaa perheenjäsenten käyttöön.
- Työntekijä vastaa hänelle annetuista tunnuksista ja salasanoista. Tunnukset ja salasanat tulee pitää aina salassa, eikä niitä saa luovuttaa muille. Salasanoissa on käytettävä vahvoja salasanoja ja suosittava

monivaiheista tunnistautumista, jos se on mahdollista. Salasanoja päivitetään ohjelmakohtaisesti sen antamien ohjeiden mukaisesti.

- Ohjelmiin ja tietoihin ei saa laittaa automaattikirjautumista. Ohjelmista kirjaudutaan aina ulos käytön jälkeen.
- Tietokone ja älylaite lukitaan aina käytön päättymisen jälkeen. Lukituksen avaamiseksi tulee olla käytössä vahva salasana.
- Työntekijä pitää tietokoneen ja muut älylaiteet päivitettyinä. Organisaation ohjeiden ulkopuolisia tiedostoja, ohjelmia tai sovelluksia laitteisiin ei saa asentaa laitteisiin ilman lupaa.
- Hävitetään henkilötietoja sisältävän materiaalin tai tarpeettomaksi jääneen tiedon oikein annettujen ohjeiden mukaisesti.
- Työntekijä on tietoinen ohjelmien lokitietojen tallentamisesta ja asiakaspalvelun saapuvien puheluiden tallentamisesta.
- Työntekijän on ilmoitettava esimiehelleen havaitsemistaan tietosuoja- ja tietoturvarikkomuksista ja puutteista. (Andreasson, Koivisto & Ylipartanen 2016, 196-199.)

Haastattelussa ilmeni, että salassapitovelvollisuus henkilötietojen käsittelijöille oli itsestään selvyys: ”Jokainen on allekirjoittanut käyttö- ja salassapitovelvollisuus-sopimuksen. Uusien työntekijöiden ja harjoittelijoiden kanssa sopimus tehdään myös heti töiden alettua”.-- ”Harjoittelijat eivät käsittele henkilötietoja, koska heillä ei ole mitään oikeuksia verkkotietojärjestelmiin. Ainoastaan työsuhteessa olevilla asentajilla on oikeudet”.

9 HENKILÖTIETOJEN KÄSITTELY KENTTÄTYÖSSÄ

Enontekiön Sähkö Oy:ssä henkilötietoja käsittelevät myös sähköverkkoasentajat erinäisten työtehtävien hoitamisessa. Tällaisia työtehtäviä ovat esimerkiksi mittareiden vaihdot ja asennukset, uusien liittymien rakentaminen sekä sähkön käyttöpaikkojen kytkentätoimenpiteet. Sähköasentajat käyttävät työtehtäviensä hoitamiseen Mitello-verkkotietojärjestelmää sekä Telian kulutusmittauspalvelua. Mittaritöitä tekevät asentajat käyttävät myös Generis-mittaustieto- ja käyttöpaikkajärjestelmä. Haastattelun avulla kartoitettiin asentajien tietämys ja taidot tietosuojan sekä tietoturvan osalta. Haastateltavat olivat anonyymejä.

Sähköverkkoasentajilta kysyttiin heidän tietämyksestään Euroopan unionin tietosuoja-asetuksesta. Sähköverkkoasentajien mielestä heidän tietämyksensä asetuksesta oli tarpeeksi hyvä heidän työnkuvaansa nähden. ”Työnantajan puolelta mitään erilliskoulutusta ei ole järjestetty, ohjeita on annettu ainoastaan suullisesti”. Ohjeistusta ja koulutusta työnantajan puolelta kaivattiin ja toivottiin. Haastattelun aikana havainnoin, että sähköverkkoasentajilla ei ollut tietoa siitä, että mitkä kaikki asiat luetaan henkilötiedoiksi. Esimerkiksi käyttöpaikkatunnusta tai mittarinnumeroa ei mielletty havaintojeni mukaan henkilötiedoksi.

Asentajilla oli hyvä asenne tietoturvan huomioimiseen työpäivän aikana. Sähköverkkoasentajat valmistautuvat ennakoiden tehtäviin, joissa henkilötietoja tarvitaan. Ennen kohteeseen menoa tarvittavat tiedot laitetaan paperille, koska sähköverkkoasentajien mukaan älylaitteella kuten puhelimella tiedot näkyvät liian pienenä. Henkilötietoja sisältävä paperi laitetaan tuhottavien papereiden keräysastiaan, kun tietoja ei enää tarvita, eli heti kohteesta saapumisen jälkeen. Tietosuoja ylläpitäminen on tehty helpoksi ohjelmien toimittajien puolesta, koska ohjelmissa ei näy kuin työtehtävien hoitamisen kannalta oleelliset tiedot. Esimerkiksi henkilötunnusta ei näy missään ohjelmassa. Mittaritöitä tekevät sähköverkkoasentajat käyttävät Generistä, jossa pystyisi näkemään kaikki asiakastiedot, mutta siellä pääsyä on rajattu käyttöoikeuksilla. Sähköasentajien tekemä henkilötietojen käsittelymäärä jäi vastaajien mukaan myös hyvin pieneksi, ainoastaan yhden tai kahden henkilön tietoja käsiteellään työpäivän aikana. ”Tämäkin vaihtelee sitten sähköverkkoasentajan tehtävän kuvan mukaan. Joillakin asentajilla

ei välttämättä ole henkilötietojen käsittelyä kuin päivystyksen aikana kerran kuukaudessa”.

Haastattelujen vastauksien perusteella tietoturvassa löytyi parannettavan varaa ja työtavoissa olisi korjattavaa. Puutteita ilmeni lähinnä tietokoneiden ja älylaitteiden lukitsemisessa ja tietokoneiden päivittämisessä. Sähköverkkoasentajat kokivat, että hei omaavat hyvät tietotekniset taidot, ja osa olisi halunnut lisäkoulutusta. Sähköverkkoasentajat tunnistivat myös hyvin erilaisia tietoturvariskejä ja osasivat nimetä hyvin työelämän tilanteita, joissa riskit voisivat konkretisoitua. Hyvänä tapana sähköasentajilla oli se, että ohjelmat sammutetaan heti käytön päätyttyä, ”ainahan ne ohjelmat suljetaan, ei niitä jätetä sinne roikkumaan”.

10 POHDINTA

Opinnäytetyön tehtiin Enontekiön Sähkö Oy:n asiakastietojen käsittelystä sekä niihin kohdistuvista riskeistä henkilötietojen käsittelijän näkökulmasta. Työtä pystyvät hyödyntämään yhtiön henkilötietojen käsittelijät, joita ovat toimiston toimihenkilöt, sähköverkkoasentajat ja yhtiön johtohenkilöt. Opinnäytetyöhön on hyvä kertaus tietosuojasta ja tietoturvasta olemassa olevalle henkilökunnalle, mutta erityisen hyödyllinen se on uusille työntekijöille. Uudet työntekijät pääsevät tutustumaan henkilötietojen käsittelyyn sekä saavat hyvän lakikatsauksen, jonka pohjalta he pystyvät syventämään tietojaan. Vaikka harjoittelijat eivät yhtiössä käsittelekään henkilötietoja, heidän on hyvä silti tutustua opinnäytetyöhön, jotta tietoturvariskit eivät realisoitusi. Harjoittelijat käyttävät kuitenkin yhtiön tietokoneita ja älylaitteita muihin tarkoituksiin, joten tietoturvan riskienhallinnan näkökulmasta myös heidän on tiedettävä perusasiat ja noudatettava yhteisiä pelisääntöjä.

Opinnäytetyö on kirjoitettu siten, että se kokonaisuutena vastaa tutkimuskysymykseen, miten Enontekiön Sähkö Oy:ssä käsitellään henkilötietoja ja kuinka siihen liittyvät riskit on huomioitu. Apututkimuskysymykset on käyty läpi teoriaosuuksissa, joissa lakeja, säädöksiä ja alan tietokirjallisuutta on käytetty vastamaamaan kysymykseen. Haastatteluissa on pohdittu riskejä ja niitä on tuotu esille myös teoriassa. Haastatteluissa ilmeni, että riskejä havainnoidaan työn aikana, mutta ne eivät ole onneksi realisoituneet. Apututkimuskysymys, kuinka tietoturva on otettu huomioon, tuli esille tietoturvaan keskittyneessä luvussa.

Henkilötietojen käsittely on tänä päivänä niin tavallista, ettei siihen mielestäni osata suhtautua sen vaatimalla vakavuudella. Kerran menetettyä henkilötietoa ei voi saada takaisin eikä rikosoikeudellisesti ole olemassa siihen sopivaa rangaistusta, koska vahinko uhrille on mittaamaton. Siksi henkilötietojen käsittelijöillä ja reksiterin pitäjillä on suuri vastuu ja velvollisuus pitää tiedot suojattuina ja ehyinä. Euroopan unionin vuonna 2016 voimaan tulleen tietosuoja-asetuksen avulla tietoja voidaan paremmin turvata. Onko tietosuoja-asetus kuitenkin vielä hieman hakusessa työntekijöiden keskuudessa? Olen itse työssäni huomannut, etteivät kaikki tahot edelleenkään ymmärrä, kuinka tietoja esimerkiksi luovutetaan turvallisesti eteenpäin.

Opinnäytetyötä varten tekemäni haastattelut osoittivatkin, että ainakin sähköverkkoasentajat, joiden pääsääntöinen työ ei ole henkilötietojen käsittelyssä tarvitsisivat enemmän tietoa tietosuojasta ja tietoturvasta. Heille tulisi järjestää heidän tarpeidensa mukaan pieniä koulutuksia, joiden avulla he saisivat työkaluja tietoturvan parantamiseen sekä muistutuksena hyviä tietosuojaohjeita. Mielestäni sähköasentajilla oli maalaisjärkeen perustuvat tavat tietosuoja-asioissa. Haastattelun aikana havainnoin myös, että tietämys siitä, mitkä tiedot luetaan henkilötiedoiksi, olivat puutteellisia. Haastattelut olivat anonyymejä, jotta työn eettisyys säilyisi. Haastatteluaineisto tuhottiin heti opinnäytetyön valmistuttua. Haastateltavat ovat myös saaneet mahdollisuuden lukea opinnäytetyön ennen sen julkaisemista.

Lait ja asetukset henkilötietojen turvaamiseksi ovat vahvoja ja mielestäni hyvin selkeitä. Tietoa muutenkin henkilötiedoista ja niiden käsittelystä on hyvin saatavilla. Kuluttajilla, joiden henkilötietoja on myös Enontekiön Sähkö Oy:n rekisterissä, kuitenkin on huono tietämys omista oikeuksistaan. Tämä asia ilmeni haastatteluiden aikana, kun henkilötietojen käsittelijöiltä kysyttiin, että käyttikö kukaan asiakas oikeuttaan tietojen tarkastamiseen. Tietävätkö asiakkaat oikeuksiaan vai tulisiko asiakkaita muistuttaa tästä. Opinnäytetyön luotettavuutta voidaan arvioida siten, että se on henkilötietojen käsittelijän tekemä ja opinnäytetyön tilaajan eli Enontekiön Sähkö Oy:n tarkastama. Haastattelut ovat toki haastateltavien omia mielipiteitä, jotka eivät ole asiantuntijalausuntoja, mutta ovat henkilötietojen käsittelijöiden antamia ja työelämän kokemukseen perustuvia.

Opinnäytetyötä kirjoittaessa itse opin paljon uutta tietosuojasta ja tietoturvasta. Työn tekeminen oli hyvin mielenkiintoista ja mukaansatempaavaa. Haluan kiittää haastateltavia, jotka antoivat työelämäkokemuksia ja empiiristä tietoa henkilötietojen käsittelystä verkkopalveluyhtiössä. Haluan myös kiittää Enontekiön Sähkö Oy:n johtoa, joka mahdollisti koko opinnäytetyön tekemisen.

LÄHTEET

Aalto-Setälä, M. Viitaila, M. 2018. Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille. Helsinki: Keskuskauppakamari.

Anrdeasson, A. & Koivitso, J. 2013. Tietoturvaa toteuttamassa. Helsinki. Tietosanoma.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki. Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016, 3.painos. Tietosuojakäsikirja johdolle. Helsinki. Tietosanoma.

Avioliittolaki 13.6.1929/234.

Bergström, E., Karhula, P. & Kipinoinen, K. 2018. Eduskunta. EU:n tietosuojauudistuksen kansallinen täytäntöönpano. Viitattu 26.4.2021 https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx

Energiateollisuus 2020. Luottamuksellisuus ja syrjimättömyys sähkömarkkinoilla. Viitattu 20.4.2021 https://energia.fi/files/4763/Luottamuksellisuus-_ja_syrjimattomyysohje_2020_final.pdf

Enerim Oy. EnerimCIS. Viitattu 22.2.2021 https://enerim.com/fi/software/enerimcis

Enontekiön Sähkö Oy 2019. Rakentajan muistilista. Viitattu 17.2.2021 https://enontekio.fi/asuminen-ja-ymparisto/enontekion-sahko-oy/rakentajan-sahkomuisto/

Euroopan parlamentin ja neuvoston asetus (EU) luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (679/2016)

Financer 2021. Pankkiasioiden hoito valtakirjalla. Viitattu 29.3.3021 https://financer.com/fi/blogi/pankkiasioiden-hoito-valtakirjalla/

Finanssivalvonta 2018. Kuolinpesän asioiden hoitaminen. Viitattu 6.4.2021 https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/kuolinpesan-asiat/

Fingrid Oyj. Mikä on Datahub?. Viitattu 22.2.2021 https://www.fingrid.fi/sahkomarkkinat/datahub/

F-Secure. 2021. Mikä on VPN?. Viitattu 26.4.2021 https://www.f-secure.com/fi/home/articles/what-is-a-vpn

Haapalehto, S. & Krakau, T. 2020. Tietopyynnöt ja henkilötietojen luovuttaminen. Hensinki. Alma Talent Oy

Hardy, K. 2015. Enterprise Risk Management A Guide For Government Professionals. A Wiley Brand. E-kirja. Luettu 30.3.2021 https://ebookcentral-proquest-com.ez.lapinamk.fi/lib/ulapland-ebooks/reader.action?docID=1794065

Helsingin yliopisto. Avoin yliopisto. Viitattu 29.3.2021 https://www.avoin.helsinki.fi/oppimateriaalit/oikeustiede/materiaali/osa3.html

Hirvonen, A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja. Luettu 23.5.2021 https://www2.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Juuti, P. & Puusa, A. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Luettu 14.2.2021. E-kirja. ISBN 978-952-345-616-7.

Jyväskylän yliopisto 2009. IP-osoite (Internet Protocol). Viitattu 26.4.2021 https://www.jyu.fi/digipalvelut/fi/ohjeet/sanasto/ip-osoite-internet-protocol

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas tunnista uhat, hallitse riskit. Talentum Media Oy.

Kirjapitolaki 30.12.1997/1336.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö.Helsinki. Alma Talent Oy.

Kuluttajaliitto. Velkaopas – Neuvoa ja apua raha-asioiden hoitoon 2017. 2. päivitetty versio. ISBN 978-952-9787-58-6. Viitattu 16.2.2021 https://www.kuluttajaliitto.fi/uploads/2020/10/a4ba1b76-velkaopas.pdf.

Kuluttajansuojalaki 20.1.1978/38.

Kyberturvallisuuskeskus. Näin keräät ja käytät lokitietoja. Viitattu 15.3.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja?toggle=Lokeja%20koskeva%20lains%C3%A4%C3%A4d%C3%A4nt%C3%B6&toggle=Lokitus%20ja%20SIEM

Laki holhoustoimesta 1.4.1999/442.

Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011

Land, M., Ricks, T & Ricks, B. 2014. Security Management A Critical Thinking Approach. Taylor & Francis Group.

Maanmittauslaitos. Liittymäsopimukset. Viitattu 29.3.2021 https://www.kiinteistoasiat.fi/help_items/advanced_information/additional_terms/content/connection_contracts?locale=fi

Nykänen, P. 2019 Miten lakia tulkitaan?. Tampereen yliopisto. Viitattu 26.4.2021 https://events.tuni.fi/uploads/2019/09/e6de95fa-miten-lakia-tulkitaan.pdf

Näveri, A. 2020. Pelkkää henkilötunnusta ja nimeä ei pitäisi käyttää ihmisten tunnistamiseen, sanoo tietosuojavaltuutettu – miksi moni taho silti kysyy tunnusta puhelimessa?. Yle 6.11.2020. Viitattu 16.3.2021. https://yle.fi/uutiset/3-11625972

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV. Tutkimuksen arviointi – reflektointia. Viitattu 26.4.2021. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_3.html

Sahala, H. 2000. Kuntaliitto. Yleiskirje 4/80/2000. Asiakkaiden omien rahavarojen käsittely sosiaali- ja terveystoimessa.

Sikanen, S. 2016. CGI. Datahub mullistaa sähköbisneksen – Mitä 10 datahub-projektia ovat opettaneet. Viitattu 22.2.2021. https://www.cgi.com/fi/fi/blogi/datahub-mullistaa-sahkobisneksen

Suomen perustuslaki 11.6.1999/731.

Suomen Standardisoimisliitto SFS ry. Viitattu 22.5.2021 https://sales.sfs.fi/fi/index/tuoteuutiset/euntietosuoja-asetusjastandardit.html.stx

Tietosuojalaki 5.12.2018/1050.

Tietosuojalautakunta päätös 1/2006.

Tietosuojatyöryhmä 2017. Asetuksen 2016/678 mukaista läpinäkyvyyttä koskevat suuntaviivat. Viitattu 8.3.2021. https://tietosuoja.fi/documents/6927448/8316711/L%C3%A4pin%C3%A4kyvyys+fi/c102605b-e386-4661-9b51-bf427875c8db/L%C3%A4pin%C3%A4kyvyys+fi.pdf

Tietosuojavaltuutetun toimisto 2021. Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. Viitattu 16.3.2021. https://tietosuoja.fi/arvioi-riskit

Tietosuojavaltuutetun toimisto 2021. Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle. Viitattu 3.3.2021 https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle

Tietosuojavaltuutetun toimisto 2021. Kun haluat tarkistaa tietosi. Viitattu 15.3.2021 https://tietosuoja.fi/kun-haluat-tarkastaa-tietosi

Tietosuojavaltuutetun toimisto 2021. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. Viitattu 30.3.2021 https://tietosuoja.fi/tietosuoja

Traficom. 228/2020. Pienyritysten kyberturvallisuusopas. Viitattu 24.3.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Tutkimuseettinen neuvottelukunta 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Viitattu 22.5.2021 https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

Valtiovarainministeriö. Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI 3/2007. Luettu 23.3.2021 https://www.suomi-digi.fi/sites/default/files/2020-06/mainbook_3_2007.pdf

Valtionvarainministeriö. Tärkein tekijä on ihminen, - henkilöstö -turvallisuus osana tietoturvallisuutta. VAHTI 2/2008. Luettu 23.3.2021 file:///C:/Users/OMISTAJA/AppData/Local/Temp/T%C3%A4rkein%20tekij%C3%A4%20on%20ihminen%20-%20henkil%C3%B6st%C3%B6turvallisuus%20osana%20tietoturvallisuutta,%20VAHTI%202_2008-1.PDF

Verkkopalveluehdot VPE 2019.

Viestintävirasto. Lokien keräys ja käyttö. 4/2016. Luettu 15.3.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitus-ohje.pdf

Vilkka, H. 2015. Tutki ja Kehitä. 4., uudistettu painos. Jyväskylä. PS-kustannus.

Voigt, P & von dem Bussche, A. 2017. The EU Genral Data Protection Regulation. E-kirja. ISBN 978-3-319-57958-0. Luettu 8.3.2021.

LIITTEET

Liite 1. Haastattelukysymykset

Liite 2. Tietosuojaseloste

Liite 3. Tietosuojan ja tietoturvan riskienhallinnan muistilappu

LIITE 1. 1(2)

HAASTATTELUKYSYMYKSET

Haastattelukysymykset henkilötietojen käsittelijöille

- Kuinka hyvin tunnet mielestäsi EU:n tietosuoja-asetuksen ja sen vaatimukset?
- Minkälainen prosessi asiakastietojen päivittäminen oli uuden asiakastietojärjestelmän ja Datahubin asettamien vaatimuksien täyttämiseksi?
- Minkälaisia puutoksia asiakastiedoissa oli ja kuinka tiedustelitte asiakkaalta esimerkiksi puuttuvaa henkilötunnusta?
- Minkälaisia riskejä huomasitte asiakastietojen täydentämisen aikana/takia?
- Kuinka hyvin saitte täydennettyä puuttuvat asiakastiedot?
- Kuinka tiedustelitte asiakkaalta puuttuvia henkilötietoja?
- Oliko asiakastietojen kysymisen yhteydessä sellaisia tilanteita, jossa asiakas kieltäytyi antamasta omia henkilötietojaan verkkopalveluyhtiölle? Kuinka toimit, jos tällainen tilanne tuli vastaan?
- Koetko, että asiakas tietää omat oikeutensa rekisteröitynä?
- Kuinka tietoisuus tai epätietoisuus ilmenevät?
- Minkälaisia ongelmia olet havainnut henkilötietojen käsittelyssä, esimerkiksi kielimuuri ulkomaalaisten asiakkaiden kanssa, haastava asiakas, kuulun ymmärtäminen ja tiedon saaminen asiakkaalta?
- Voiko asiakaspalvelija omalla toiminnallaan minimoimaan tietosuoja ja tietoturvariskejä? Kuinka näitä riskejä voidaan minimoida?
- Fyysisen asiakaspalvelun tietosuojariskit?
- Tietojen oikeudellisuuden takaaminen? Mistä tiedän, että asiakas antaa oikeat henkilötiedot?

LIITE 1. 2(2)

Haastattelukysymykset sähköverkkoasentajille

- Onko EU:n tietosuoja-asetus sinulle tuttu?
- Onko työnantaja antanut sinulle tietoa tietoturvasta ja tietosuojasta?
- Onko ohjeistus ollut mielestäsi riittävää?
- Kuinka huomioit tietoturvan työpäivän aikana?
- Puututko ja raportoitko esimiehelle, jos huomaat tietoturvassa aukkoja tai parantamisen varaa?
- Kuinka olet suojannut työpaikan työlaitteen?
- Minkälaiset tietotekniset taidot omaat?
- Kuinka hyvin tunnet erilaiset tietoturvariskit?
- Kuinka suojaat asiakastietoja työpäivän aikana?
- Minkälaisia henkilötietoja käytät/tarvitset työtehtävän suorittamiseen?
- Näetkö verkkotietojärjestelmän kautta asiakkaasta sellaista tietoa, jota et tarvitse työtehtävän hoitamiseen?
- Mitä henkilötietoja tarvitset työtehtävän hoitamiseen?
- Kuinka paljon käsittelet henkilötietoja työpäivän aikana ja missä tilanteessa henkilötietojen käsittely tapahtuu?

LIITE 2. 1(3)

ENONTEKIÖN SÄHKÖ OY:N ASIAKASTIETOREKISTERI

REKISTERINPITÄJÄ JA YHTEYSHENKILÖ

Enontekiön Sähkö Oy

y-tunnus 1571816-2

Osoite: Ounastie 165, 99400 Enontekiö

Muut yhteystiedot: +358 (0) 16 3316575, enontekionsahko@neve.fi

Yhteyshenkilö: Mikko Veima

Yhteyshenkilön yhteystiedot: +358 40 182 7245, mikko.veima@neve.fi

HENKILÖTIETOJEN KÄSITTELYN TARKOITUS

Enontekiön Sähkö Oy ja sen valtuuttamat yhteistyökumppanit keräävät ja käsittelevät rekisteröityjen henkilötietoja seuraaviin käyttötarkoituksiin:

- Asiakkuuksien luomiseen, hoitamiseen ja kehittämiseen
- Asiakkuuksien tunnistamiseen
- Lakisääteisten tehtävien hoitamiseksi sekä palveluiden ylläpitoon ja kehittämiseen
- Maksujen valvontaan ja perintään
- Asiakasviestintään

KÄSITTELYN OIKEUSPERUSTE

Henkilötietojen käsittelyn oikeusperustana on Enontekiön Sähkö Oy:n ja asiakkaan välinen sopimussuhde tai sopimusta valmistelevien asiakastietojen kerääminen. Henkilötietojen käsittely perustuu Enontekiön Sähkö Oy:n ja sen asiakkaan väliseen asiakassuhteeseen. Henkilötietoja käsitellään asiakassuhteen oikeuksien ja velvollisuuksien täyttämiseksi. Käsittely perustuu myös lakisääteisen velvoitteen täyttämiseen, joita löytyy kirjanpito- ja sähkömarkkinalainsäädännöstä sekä viranomaispäätöksistä. Henkilötietoja käsitellään suomaista lainsäädäntöä sekä Euroopan unionin tietosuoja-asetuksen mukaisesti.

REKISTERIN TIETOSISÄLTÖ

Tietoja kerätään asiakkaalta yllä mainittujen tarkoitusten täyttämiseksi. Laajimmillaan tämä tarkoittaa seuraavien tietojen keräämistä ja tallentamista:

LIITE 2. 2(3)

- Asiakkaasta kerättävät tiedot: nimi, henkilötunnus, osoite, puhelinnumero, sähköpostiosoite
- Käyttöpaikan tiedot: osoite, sähkön kulutusarvio, lämmitysmuoto, mittaustapa, pääsulakekoko, laitetiedot
- Laskutus ja maksukäyttäytymistiedot: laskutusosoite, laskutusrytmi, maksutiedot, laskutustapa
- Asiakkaan ja Enontekiön Sähkö Oy:n väliset tallennetut puhelut
- Muut asiakkaan tai mahdollisen uuden asiakkaan suostumuksella saadut tiedot, jotka ovat tarpeellisia asiakkuuden hoitamiseksi

Perustietojen ja laskutukseen liittyvien tietojen antaminen on rekisteröidyn asiakkuuden hoitamisen kannalta oleellista. Lakisääteisten velvoitteiden täyttämisen kannalta esimerkiksi energian kulutustietoja verkkopalveluyhtiön on kerättävä asiakkuudesta. Enontekiön Sähkö Oy ei pysty tarjoamaan kaikkia palveluitaan, jos vaaditut tiedot puuttuvat asiakkuudesta.

TIETOJEN SÄILYTYSAIKA

Verkkopalvelusopimukset, pientuotantosopimukset sekä liittymäsopimukset poistetaan 10 vuoden kuluttua sopimuksen päättymispäivästä. Puhelutallenteet säilytetään kaksi vuotta puhelusta.

TIETOLÄHTEET

Tiedot asiakkaista saadaan pääsääntöisesti asiakkaalta itseltään tarjouspyyntöjen, tilausten, sopimusten ja muiden kontaktien yhteydessä. Tietoja saadaan myös asiakkaiden käyttämien palveluiden ja tuotteiden käytöstä. Asiakastietoja voidaan päivittää ja kerätä myös osoite- ja päivityspalveluiden tai muun vastaavan palveluntarjoajan rekistereistä. Tietoja voidaan päivittää myös energiateollisuuden sähkömarkkinoiden tiedonvaihdon sääntöjen perusteella.

TIETOJEN LUOVUTUS

Enontekiön Sähkö Oy:n asiakasrekisteristä ei lähtökohtaisesti luovuteta tietoja eteenpäin. Lainsäädännön mukaan tietoja voidaan luovuttaa viranomaisille. Tietoja voidaan siirtää Enontekiön Sähkö Oy:n yhteistyökumppaneille, palveluntuottajille ja alihankkijoille. Näitä tahoja ovat mm. mittauspalveluntuottajat, perintätoimistot ja tulostusoperaattorit. Tietoja ei siirretä EU:n tai ETA:n ulkopuolelle

LIITE 2. 3(3)

REKISTERÖIDYN OIKEUDET

Rekisteröidyllä on oikeus:

- tarkistaa rekisteriin tallennetut tiedot
- oikaista virheellinen tai puutteellinen tieto
- siirtää tiedot toiseen järjestelmään
- rajoittaa tietojensa käsittelyä
- tulla unohdetuksi
- tehdä valitus valvovalle viranomaiselle, eli Tietosuojavaltuutetulle

Asiakas voi harjoittaa oikeuksiin ottamalla yhteyttä Enontekiön Sähkö Oy:n asiakaspalveluun.

Enontekiön Sähkö Oy

Ounastie 165, 99400 Enontekiö

puh: +358 (0)16 3316575, enontekionsahko@neve.fi

Tietosuojavaltuutetun toimisto

PL 800, 00531 Helsinki

puh: 02 9566 6700, tietosuoja@om.fi

LIITE 3. 1(4)

MUISTILISTA HENKILÖKUNNALLE

PERUSPERIAATTEET

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- Käsittelylle oltava laillinen peruste ja tietoja käsitellään oikein sekä rekisteröidyn informoiminen

Käyttötarkoitussidonnaisuus

- Tietoja kerätään ja käytetään ainoastaan yhtiön nimenomaista ja lakisääteistä tehtävien hoitamiseksi

Tietojen minimointi

- Asiakuudesta kerätään ainoastaan vaadittava tieto henkilötunnus, nimi, osoite, yhteystiedot, laskutusosoite ja käyttöpaikan tiedot

Säilytyksen rajoittaminen

- Säilytetään Kirjanpitolain mukaisesti 10 vuotta sopimuksen päättymisestä

Eheys ja luottamuksellisuus

- Tietoja käsitellään asianmukaisella tavalla, turvallisesti siten, ettei tieto vaarannu missään käsittelyn kohdassa tai ettei se päädy vääriin käsiin

Salassapitovelvollisuus

- Kaikkia työntekijöitä sitoo salassapitovelvollisuus ja tiedon hyväksikäyttökielto

REKISTERÖIDYN OIKEUDET

Oikeus saada pääsy tietoihin

- Tietopyyntöön vastataan lähettämällä asiakkaalle tietosuojaraportti hänen haluamallaan tavalla

Oikeus tiedon oikaisemiseen ja poistamiseen

- Vastaanotamme mielellämme oikaisupyyntöjä, oikaisut tehdään suoraan järjestelmään. Asiakastietoja voidaan poistaa vasta säilytysajan umpeuduttua

LIITE 3. 2(4)

Oikeus omien tietojen käsittelyn rajoittamiseen

- Käyttöoikeuksien rajaaminen

Oikeus siirtää tiedot järjestelmästä toiseen

- Esimerkiksi muuttotilanteessa toiselle verkkopalveluyhtiölle

Oikeus tehdä valitus valvontaviranomaiselle

- Ohjataan asiakas Tietosuojavaltuutetun toimistolle valituksen tekemiseen

REKISTERINPITÄJÄN VELVOLLISUUDET

Rekisteröidyn informointi

- Toimitettava henkilötietojen käsittelyä koskevat tiedot eli rekisteriseloste

Rekisteriseloste

- Löytyy yhtiön internetsivuilta

Osoitusvelvollisuus

- Esimerkiksi henkilökunnan koulutus ja ohjeistus, prosessikuvaukset, dokumentointi yms.

TIETOTURVASTA

Tietojen käsittely

- Tulosteita ja sähköisiä tallenteita käsitellään aina huolellisesti. Tulosteet arkistoidaan arkistointisuunnitelman mukaisesti ja tarpeeton paperi tuhotaan keräämällä se keräysastioihin. Sähköiset tallenteet tallennetaan ainoastaan hyväksyttyihin paikkoihin.

Tietojen lähettäminen

- Sähköpostilla ei lähetetä henkilötietoja sisältäviä viestejä. Käytetään turvasähköpostia tai yhtiön pilvipalvelua.

Tietokoneet ja älylaitteet pidetään päivitettynä

- Uudet päivitykset tehdään heti kun ne ovat saatavilla. Vanhat ohjelmat ovat tietoturvariski.

LIITE 3. 3(4)

Puhtaan pöydän periaate

- Työpöytä ja työhuone ovat siistit, henkilötietoja tai muita salassa pidettäviä tietoja ei saa olla näkyvissä. Puhtaanpöydän periaate käytössä kaikissa yhtiön tiloissa.

Tietojen kalastelu

- Sähköpostien ja internetsivujen avaamisessa tulee käyttää harkintaa.

Ilmoitusvelvollisuus

- Kaikista tietoturvaloukkauksista tai -epäilyistä tulee ilmoittaa heti omalle esimiehelle

Tietokone ja älylaitteet tulee suojata

- Näyttö suojataan tietosuojakalvolla, tietokone pidetään lukittuna kun sitä ei käytetä, salasanat ja käyttäjätunnukset tulee pitää vain omana tietona. Tunnistautumisessa tulee suosia vahvaa tunnistautumista.

Tunnista ympäristösi

- Huomio työympäristösi esimerkiksi puhuessasi puhelimeen. Ulkopuolinen voi kuulla tai nähdä salassa pidettäviä tietoja.

Valvonta

- Valvonta on jokaisen työntekijän vastuulla. Ilmoita esimiehellesi, jos huomaat rikkeitä tai laiminlyöntiä työyhteisössäsi

ETÄTÖISTÄ

Tietokoneet ja älylaitteet

- Vain yhtiön tietokoneilla ja älylaitteilla tehdään töitä. Älä luovuta työvälineitä perheenjäsenten käyttöön. Älä käytä yhtiön työlaitteita omien henkilökohtaisten töiden hoitamiseen.

Tunnista ympäristösi

- Huomio työympäristösi esimerkiksi puhuessasi puhelimeen. Ulkopuolinen voi kuulla tai nähdä salassa pidettäviä tietoja.

LIITE 3. 4(4)

Vältä paperisia asiakirjoja

- Pyri välttämään paperisten asiakirjojen tuominen tai tulostaminen etätyöpisteellä. Säilytä välttämätön paperiasiakirja aina lukitussa tilassa.

  Hävitä ja arkistoi paperiset asiakirjat annettujen ohjeiden mukaisesti niin piaan kuin mahdollista.

VPN-yhteys

- Internettiä selataan ainoastaan VPN-yhteyden kautta.