Mari Mäntysalmi

EU:n tietosuojauudistus: Virhydro Oy

Opinnäytetyö

Opinnäytetyö
Kevät 2018
SeAMK Liiketoiminta ja kulttuuri
Tradenomi (AMK), Liiketalous

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Liiketoiminta ja kulttuuri

Tutkinto-ohjelma: Tradenomi (AMK), Liiketalous

Suuntautumisvaihtoehto: Henkilöstöhallinto ja johtaminen

Tekijä: Mäntysalmi Mari

Työn nimi: EU:n tietosuojauudistus: Virhydro Oy

Ohjaaja: Sippola Petra

Vuosi: 2018 Sivumäärä: 42 Liitteiden lukumäärä: 4

Tämä opinnäytetyö selvittää Euroopan parlamentin ja neuvoston julkistamaa uutta tietosuoja-asetusta (EU 2016/679), koskien henkilötietojen parempaa suojaamista. Tietosuoja-asetusta tulee lain mukaan noudattaa 25.5.2018 alkaen, jolloin tietoturvatoimenpiteiden on oltava asetuksessa vaadittavaa tasoa. Nykypäivänä globalisaatio ja teknologian kehitys etenevät niin nopeasti, että henkilötietojen tiukemmalle suojaamiselle on syynsä. Yksityisyyden suoja on korostunut, ja yksityishenkilöiden oikeuksista halutaan pitää tiukemmin kiinni. Tietosuoja-asetuksen avulla mahdollistetaan se, ettei henkilötietoja pystytä laillisesti keräämään, käsittelemään tai säilyttämään ilman, että rekisteröity olisi asiasta tietoinen.

Tietosuoja-asetuksella on merkittäviä vaikutuksia yritysten, yhdistysten sekä organisaatioiden toimintaan henkilötietojen käsittelyn kannalta. Kaikkien yllämainittujen, jotka jotenkin pitävät hallussaan mitä tahansa jäsenneltyä henkilötietoja sisältävää rekisteriä, tulee saattaa tietoturvansa asetuksen vaatimalle tasolle. Opinnäytetyössä kohdeyrityksenä on teknisen alan kauppa Virhydro Oy, jonka tietoturvatoimenpiteiden muutoksia on tämän työn myötä lähdetty toteuttamaan.

Tietosuoja-asetus on laadittu kansainvälisten ihmisoikeussopimusten sekä Euroopan unionin perusoikeuskirjaan pohjautuen. Asetusta sovelletaan suoraan lainsäädäntöön kaikissa jäsenmaissa, ja jos jäsenmaista tapahtuu laillista tietojen siirtoa kolmansiin maihin, tulee myös niissä tietoturvan olla tietosuoja-asetuksen vaatimalla tasolla. Näin jäsenmaissa tietosuojan taso on taattu yhtenäiseksi sekä turvalliseksi.

Avainsanat: EU:n tietosuojauudistus, tietoturva, tietosuoja, henkilötieto, rekisteröinti, henkilötietorekisteri

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: Business and Culture

Degree programme: Business Management

Specialisation: Human Resource Management

Author: Mäntysalmi, Mari

Title of thesis: The EU Data Protection Reform: Case Virhydro Oy

Supervisor: Petra Sippola

Year: 2018 Number of pages: 42 Number of appendices: 4

This thesis investigates the regulation reform (EU 2016/679) related to collecting and processing personal data in the area of the European Union. The European Parliament and Council have published a new regulation about the protection of the natural person's rights in processing their personal data. The regulation reform was published on 27 April 2016, and all of the EU countries should apply the reform by 25 May 2018. The priority of this regulation reform is to make sure that privacy protection remains constant in all the countries belonging in the European Union. The aim is that the natural person should always be conscious of their personal data collected or used by companies, associations, or organizations.

The regulation (EU 2016/679) should be observed by all the companies, associations or organizations processing personal data. In this thesis, the focus is on the operations and changes that will be carried out at the technical retail store Virhydro Oy.

The regulation reform is based on the UN Convention on Human Rights and on the EU Charter of Fundamental Rights. The companies, associations and organizations in the area of the European Union must also be aware of it when transferring data to countries outside the EU. They have the responsibility to ensure that the data is always be processed at the same security level as in the EU.

Keywords: EU data protection reform, privacy protection, data protection, personal data, personal data file

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

1 JOHDANTO

Euroopan unioni on 27.4.2016 julkaissut uuden tietosuoja-asetuksen (EU 2016/679), jotta henkilötietojen käsittely EU-jäsenmaissa olisi yhtenäisempää ja turvallisempaa. Tässä opinnäytetyössä perehdytään uuteen tietosuoja-asetukseen, joka koskee kaikkia henkilötietoja jotenkin käsitteleviä yrityksiä, yhdistyksiä ja muita yhteisöjä. Uusi tietosuoja-asetus korvaa vuonna 1995 säädetyn henkilötietodirektiivin (D 95/46/EY) sekä Suomen henkilötietolain (L 22.4.1999/523) niiltä osin, kuin ne henkilötietojen käsittelyä koskevat (Andreasson, Riikonen & Ylipartanen 2017, 37). Tietosuojauudistuksen on tarkoitus saada tietoturvan taso samanlaiseksi kaikissa jäsenmaissa sekä pitää tietoturva ajantasaisena teknologian kehityksen sekä globalisaation myötä. Uusi laki on astunut voimaan 25.5.2016 ja sitä aletaan soveltamaan jäsenmaissa viimeistään 25. toukokuuta 2018. (Talus ym. 2017, 9.)

Kahden vuoden siirtymäaikana rekisterinpitäjillä on ollut aikaa varautua asetuksen voimaantuloon. Asetusta tulee noudattaa tarkoin, sillä tietosuojarikkomuksesta voidaan määrätä hallinnollisia sakkoja valvontaviranomaisen toimesta (Talus ym. 2017, 9). Aihe on ajankohtainen jokaisessa yrityksessä tällä hetkellä. Suomen hallitus on 1.3.2018 jättänyt eduskunnalle esityksen Suomen tietosuojalaista (HE 9/2018), joka yhdessä EU:n tietosuoja-asetuksen kanssa on ohjenuorana rekisterinpitäjille. Lakia ei kuitenkaan ole vielä hyväksytty, joten tietoturvamuutokset on tehtävä EU:n tietosuoja-asetuksen pohjalta.

Opinnäytetyössä tarkastellaan EU:n tietosuojauudistuksen vaikutuksia teknisen alan yrityksen Virhydro Oy:n näkökulmasta. Yrityksessä ei vielä olla reagoitu uuteen tietosuoja-asetukseen. Tämän opinnäytetyön tarkoitus on, että yritys saisi laaditun selvityksen toimenpiteistä, joiden mukaan siellä tulee tietosuojan suhteen menetellä. Asetuksen mukaiseen yritystoimintaan pyrkiessä on muutoksia tehtävä tietojen käsittelyprosesseihin ja tietoturvakäytäntöjä on muutettava.

1.1 Työn tavoite ja rajaus

Virhydro Oy:lla on tarve suunnitelmalle uutta tietosuoja-asetusta varten. Sen tulee reagoida tietosuoja-asetuksen vaikutuksiin ja muutoksiin sekä saada oma toimintansa siihen tilaan, että vaaraa sanktioille ei synny. Parannetut tietosuojatoimenpiteet myös lisäävät luottamusta yrityksen asiakkaisiin ja henkilöstöön nähden. Tutkimusongelman ratkaisemiseksi tarvitaan henkilökohtaisia tiedonantoja yrityksen johdolta kehityshankkeen edistämiseksi sekä perehtymistä aiheeseen liittyviin julkaisuihin sekä kirjallisuuteen.

Opinnäytetyö on rajattu tutkimaan tietosuojauudistusta Virhydro Oy:n näkökulmasta. Siinä perehdytään myös teoreettisesti olennaisimpiin seikkoihin uudistusta koskien, mutta pääpaino on tietoturvatilanteen teoreettisen puolen tarkastelu kyseisen yrityksen kannalta ja sen pohjalta laadittava suunnitelma kunnes uuden lain siirtymäaika päättyy.

1.2 Työn rakenne

Toisessa luvussa käsitellään EU:n tietosuojauudistuksen teoreettista puolta ja tavoite siinä on tiivistää tietosuojauudistus mahdollisimman ytimekkääseen ja ymmärrettävään muotoon. Yritysesittelyssä tarkastellaan Virhydro Oy:n perustietoja sekä sen tietosuojatilannetta tällä hetkellä nykytila-analyysin sekä riskianalyysin avulla. Tarkastelu tapahtuu opinnäytetyön tekijän omien havaintojen kautta hänen työskennellessään yrityksessä, sekä haastattelemalla yrityksen toimitusjohtajaa ja henkilötietoja käsittelevää toimistoassistenttia. Neljännessä luvussa pohditaan Virhydro Oy:ta koskevia pykäliä tietosuojauudistuksen kannalta, sekä laaditaan konkreettinen suunnitelma yritykselle käsittäen kaikki henkilötiedot asiakasrekisteristä henkilöstörekisteriin ja verkkokauppaan. Tämän jälkeen käydään läpi vielä pohdinta liittyen muutoksiin tietoturvaa koskien Virhydrossa, sekä millaisia vaikutuksia niillä todennäköisesti tulee yrityksessä olemaan ja kuinka käyttöönotto toteutetaan.

2 EU:N TIETOSUOJA-ASETUS

EU:n yleistä tietosuoja-asetusta tulee 25.5.2018 lähtien noudattaa kaikissa EU-jäsenmaissa, ellei kansallisen liikkumavaran turvin ole erikseen säädetty poikkeamia (Andreasson ym. 2017, 28). Kansallinen liikkumavara tarkoittaa, että jäsenvaltiot voivat tietyissä kysymyksissä tarkentaa asetuksen säännöksiä, sekä jossain määrin myös poiketa velvoitteista (Talus ym. 2017, 36). Muutoin asetuksen on suoraan sovellettava lainsäädäntöä kaikissa EU:n jäsenmaissa (Tietosuojalait 2016, 5). Suomessa ei kuitenkaan ole säädetty kansallista liikkumavaraa, mutta hallituksen esitys eduskunnalle (HE 9/2018) on suunniteltu nimettävän tietosuojalaiksi, joka toimisi tietosuoja-asetusta täydentävänä lainsäädäntönä (Sjöblom 2018). Lakiesitystä ei vielä ole hyväksytty. Tietosuoja-asetus koskee kaikkia organisaatiota, yhdistyksiä ja muita yhteisöjä, jotka jollain tapaa käsittelevät henkilötietoja (Talus ym. 9).

EU:n tietosuoja-asetuksen mukaan henkilötiedoilla tarkoitetaan tietojen perusteella tunnistettavaan henkilöön liittyviä tietoja. Näitä ovat esimerkiksi nimi, osoite, henkilötunnus, puhelinnumero, sähköposti tai sijaintitiedot. (Andreasson ym. 2017, 30.) Suomen laista tietosuoja-asetus korvaa henkilötietolain (Andreasson ym. 29), joka kuitenkin vastaa suurilta osin uuden asetuksen sisäänrakennetun ja oletusarvoisen tietosuojan huolellisuusvelvoitetta (Talus ym. 2017, 14). Vanha henkilötietodirektiivi (D 95/46/EY) Euroopan parlamentilta sekä neuvostolta jää syrjään ja uusi asetus korvaa sen perustuen kansainvälisiin ihmisoikeussopimuksiin ja EU:n perusoikeuskirjaan (Andreasson ym. 28–29). Perusoikeuskirjasta löytyvän 7 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan niin, että hänen yksityis- ja perhe-elämänsä, kotinsa ja viestinsä saavat pysyä suojattuina (Euroopan unionin perusoikeuskirja 2012, 7 & 8 art.).

Tietosuoja-asetuksen on tarkoitus olla ohjenuorana rekisterinpitäjälle, joka käsittelee henkilötietoja. Asetuksessa on tavoitteena, että rekisteröidyn oikeudet ja vapaus pysyvät arvossaan. (Talus ym. 2017, 12.) Yleisten tietosuojaperiaatteiden mukaan tietojen tulee olla lainmukaisia, kohtuullisia ja läpinäkyviä. Niissä tulee käydä ilmi käyttötarkoitussidonnaisuus, eikä tietoja tulisi kerätä turhaan tai ylimääräistä, eikä tarpeettomia henkilötietoja tulisi säilöä turhaan tai liian pitkää aikaa. Tietojen tulee

olla täsmällisiä, eheitä ja luottamuksellisia ja säilytystä tulee rajoittaa. Rekisterinpitäjällä on myös osoitusvelvollisuus valvontaviranomaiselle. (Talus ym. 12.) Tämä tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan, että yllämainittuja asetuksen mukaisia periaatteita noudatetaan. Näin ollen on suotavaa suunnitella kaikki tietoturvatoiminnot tarkoin, sekä pitää kirjaa kaikista tietoturvaan liittyvistä tapahtumista. Lain rikkomisesta voidaan rangaista sakoilla. (Talus ym. 12.)

2.1 Henkilötietojen käsittelyyn oikeuttavat seikat

Henkilötietorekisteri on mikä tahansa tietojoukko, joka sisältää jäsenneltyä henkilötietoa. Tietosuoja-asetus ei koske yksityisten kokoamia mahdollisia rekistereitä. (Sjöblom 2018.)

Henkilötietojen käsittelyn uuden asetuksen mukaan tulee vähintään kuuden seuraavista kuvailluista edellytyksistä täyttyä (Yrittäjän tietosuojaopas 2018, 9).

Henkilön antama *suostumus* tarkoittaa, että rekisterinpitäjä on saanut rekisteröidyltä dokumentoidun luvan käsitellä tietojaan (Yrittäjän tietosuojaopas 2018, 10). Lisäksi suostumuksen on oltava selvästi henkilön itse antama, eli vaikeneminen, jonkun asian tekemättä jättäminen tai valmiiksi rastitettu ruutu eivät ole laillisia suostumuksen keräämismenetelmiä. Lasten tietoja käsiteltäessä alle 16-vuotiaan tietoja saa käsitellä vain huoltajan luvalla. Alle 16-vuotiaalle ei myöskään saa tarjota mitään tietoyhteiskunnan palveluja, eli etänä, sähköisesti, pyynnöstä tai vastiketta vastaan tarjottavia palveluja. (Yrittäjän tietosuojaopas 10.)

Oikeutettu etu on selkeä syy käsitellä henkilötietoja. Tämä voi tarkoittaa, että rekisterinpitäjän ja rekisteröidyn välillä on järkevä suhde, kuten asiakkuus, työsuhde tai jokin jäsenyys. (Yrittäjän tietosuojaopas 2018, 10). Vaikka käsittelee henkilötietoja oikeutetun edun takia, tulee käsittelyssä muistaa rekisteröidyn perusoikeudet ja noudattaa niitä, sekä tietojen käyttötarkoitussidonnaisuutta. Lasten tietojen käsittelyä koskee tässäkin tapauksessa tarkemmat perusoikeudet ja vapaudet, jotka saattavat estää tietojen käsittelyn niissä määrin, kuin olisi tarpeellista (Yrittäjän tietosuojaopas 10).

Rekisteröidyn ja rekisterinpitäjän välinen sopimus voi antaa rekisterinpitäjälle luvan käsitellä henkilötietoja ja luovuttaa niitä kolmansille osapuolille (EU 2016/679, 28 art. 4 kohta). Esimerkiksi jätehuollossa rekisterinpitäjän on luovutettava rekisteröidyn osoitetiedot aliurakoitsijalle, jotta aliurakoitsija voi käydä tyhjäämässä jätekaivot. Tässä tapauksessa sopimus syntyy, kun henkilö sopii jätehuollosta. Kuitenkin rekisterinpitäjä, eli tässä tapauksessa jätehuolto, on vastuussa, että myös aliurakoitsija käyttää tietoja käyttötarkoitukseen soveltuvin tavoin ja henkilötietoasetuksen mukaisesti (EU 2016/679, kohta 81).

Lakisääteinen velvoite on pätevä peruste käsitellä henkilötietoja ilman erillistä rekisteröidyn suostumusta (Yrittäjän tietosuojaopas 2018, 11). Lakisääteinen peruste tarkoittaa siis tietojen käsittelyä yleisen edun vuoksi tai julkisen vallan käyttämiseksi (EU 2016/679, kohta 45). Lakisääteinen velvoite koskee esimerkiksi tietojen toimittamista verottajalle tai tulliin tai talousrikosten tutkintaan tarvittavia tietoja esimerkiksi rahoitusyhtiöiltä.

Elintärkeä tai yleinen etu antavat myös oikeuden käsitellä henkilötietoja (Yrittäjän tietosuojaopas 2018, 11). Tämä koskee siis tilanteita, joissa voidaan säästää ihmishenkiä. Esimerkiksi johonkin elintarvike-erään on voinut joutua hengenvaarallista ainetta ja valmistaja pyytää myyjältä tiedot kaikista tuotteen ostajista ja ilmoittaisi heille esimerkiksi puhelimen välityksellä vaarallisesta elintarvikkeesta. Tällöin myyjä luovuttaa tietoja kolmannelle osapuolelle, jolle ne muussa tilanteessa eivät periaatteessa kuulu.

Julkinen valta saa käsitellä henkilötietoja, mutta EU:n tietosuoja-asetuksen mukaan jokaisen jäsenvaltion tulisi oman lainsäädäntönsä nojalla määritellä, mitkä toimet ja tehtävät julkinen valta käsittää (EU 2016/679, kohta 50).

2.2 Rekisterinpitäjän ja henkilötietojen käsittelijän roolit

EU:n tietosuoja-asetuksessa osoitetaan, että rekisterinpitäjä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (EU 2016/679, 4 art. 7 kohta). Henkilötietojen

käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (EU 2016/679, 4 art. 8 kohta). Tämä merkitsee, että yritys voi olla yhtä aikaa rekisterinpitäjä sekä henkilötietojen käsittelijä. Esimerkiksi IT-palveluita tarjoava yritys voi toimia rekisterinpitäjänä omien asiakkaidensa kohdalla, mutta käsitellessään asiakkaidensa loppuasiakkaita asiakkaan määräysten mukaisesti ja lukuun, toimii yritys tällöin henkilötietojen käsittelijänä. (Hanninen ym. 2017, 24–25.) Lisäksi esimerkiksi ulkoistettu kirjanpitäjä tai palkanlaskija on yrityksen henkilötietojen käsittelijä, kun yritys on rekisterinpitäjä.

Uusi asetus muuttaa yrityksien toimintoja myös niin, että rekisterinpitäjän on pystyttävä vaadittaessa osoittamaan käsittelevänsä henkilötietoja lain mukaisesti (Sjöblom 2018). Aikaisemmin henkilötietolain mukaan on riittänyt, että lakia noudatetaan, mutta tietosuojauudistuksen myötä tulee rekisterinpitäjän pystyä se osoittamaan (Sjöblom). Tämä tarkoittaa osoitusvelvollisuutta, eli kaikista henkilötietojen käsittelyistä tulee pitää dokumentaatiota (Andreasson, ym. 2017, 143). Henkilötietojen käsittelijä on myös velvoitettu ilmoittamaan merkittävistä tietoturvaloukkauksista rekisterinpitäjälle, joka on velvoitettu kertomaan valvontaviranomaiselle sekä rekisteröidylle 72 tunnin kuluessa sen ilmitulosta (EU 2016/679, 33 art. 1 kohta). Uudistuksen valvontaviranomaisena toimii tietosuojavaltuutettu (Tietosuojavaltuutetun toimisto, 1.3.2018).

Hanninen ym. (2017, 25) huomauttavat, että käsittelytilanteissa tulee huomioida, mikä taho määrittelee henkilötietojen tarkoitukset ja keinot. Tilanteessa, jossa yritys toimii rekisterinpitäjänä ja tarjoaa työntekijöilleen hierontapalveluja työsuhde-etuna, voidaan hierontapalveluja tarjoava yritys tai toiminimi myös todeta rekisterinpitäjäksi, toimien samalla myös henkilötietojen käsittelijänä. Tämä tarkoittaa, että hierontayritys tai toiminimi voi käyttää henkilötietoja palvelujen tarjoamiseksi sekä esimerkiksi asiakashallintaan (Hanninen ym., 25). Hierontayritys tai toiminimi on laillisesti oikeutettu käyttämään rekisterinpitäjältä saamiaan henkilötietoja, sillä rekisterinpitäjäyritys saa luovuttaa työntekijöidensä tiedot edellyttäen, että luovuttaminen koskee muun muassa työterveyttä tai työhön kuuluvia etuja. EU:n tietosuoja-asetuksen (EU 2016/679) alkuosan 155 kohdassa todetaan työntekijöiden tietojen käsittelyyn oikeuttaviksi seikoiksi, että tiedot liittyvät työhön tai työntekijä on antanut

suostumuksensa käsittelyyn, tietoja tarvitaan palvelukseen ottamista tai työsopimuksen täytäntöönpanoa varten tai työn suunnitteluun ja organisointiin, yhdenvertaisuuden ja monimuotoisuuden toteutumisen ylläpitämiseen työpaikalla, työturvallisuuteen tai työntekoon liittyvien oikeuksien ja etuuksien yksilölliseen tai kollektiiviseen käyttöön tai työsuhteen päättämiseen.

2.3 Tietosuojavastaava

Tietosuojavastaava yrityksessä on henkilö, joka valvoo henkilötietojen käsittelyä (Tietosuojavaltuutetun toimisto 2018). Tietosuojavastaava tulee nimittää, kun rekisterinpitäjä on julkishallinnon toimija tai sen ydintehtävät koostuvat henkilötietojen käsittelystä, tai kun henkilötietojen käsittely on laajamittaista ja sisältää arkaluontoisia henkilötietoja tai erityisryhmiin kuuluvien henkilötietoja.

Kaikkien yrityksien ei tarvitse nimetä tietosuojavastaavaa, elleivät yllämainitut vaatimukset täyty, mutta jokaisen henkilötietoja käsittelevän yrityksen kannattaa nimetä tietosuojavastaavaa vastaava henkilö (Tietosuojavaltuutetun toimisto 2018). Tietosuojavastaavan toiminnot voi myös ulkoistaa.

2.4 Rekisteröidyn oikeudet

Henkilötietojen keräämistä suunnitellessa tulee huomioida oikeudet, jotka rekisteröidyllä on. Rekisteröidyllä on oikeus saada tieto siitä, onko hänen henkilötietojaan käsitelty tai jos ei ole, niin todiste siitä (EU 2016/679, 15 art.). Rekisteröidyllä tulee olla pääsy omiin henkilötietoihinsa niin halutessaan. Hänellä on oikeus saada tietoonsa tietojen käsittelyn tarkoitukset sekä henkilötietoryhmät, joihin hän kuuluu. Lisäksi oikeus velvoittaa, että rekisteröidylle pitää pystyä ilmaisemaan määritelty ajanjakso, kuinka kauan henkilötietoja aiotaan säilyttää tai ainakin kriteerit, kuinka ajanjakso määritellään. Rekisteröidyllä on oikeus pyytää rekisterinpitäjää korjaamaan virheelliset tiedot. (EU 2016/679, 15 art.) Rekisteröidyn oikeuksiin sisältyvät myös oikeus rajoittaa tietojen käsittelyä sekä oikeus siirtää tietonsa toiseen järjestelmään, mikäli se teknisesti on mahdollista (18 art. & 20 art.). Rekisterinpitäjän tulee myös huolehtia, että jos se on välittänyt henkilötietoja sopimusten puitteissa joillekin muille

rekisterinpitäjille, tulee myös näiden pystyä tiedot poistamaan ja olla poistamisesta tietoisia rekisteröidyn niin vaatiessa. Rekisterinpitäjällä tulee siis kyetä jäljittämään välittämänsä tiedot. (17 art.)

Rekisteröidyllä on oikeus tulla unohdetuksi. Näin ollen kaikki tieto, jota rekisteröidystä on kerätty, pitäisi pystyä rekisteröidyn näin halutessa poistamaan. (EU 2016/679, kohta 66.) Lisäksi rekisteröidyllä on oikeus saada tietoonsa kaikki hänestä kerätty tieto (kohta 63). Jos tietoja pimitetään tai rekisteröity muuten kokee tulleensa loukatuksi vastoin Euroopan Unionin asetusta, on rekisteröity velvollinen ja oikeutettu ilmoittamaan valvontaviranomaiselle. Valvontaviranomaisen tulisi ilmoittaa rekisteröidylle käsittelyn etenemisestä ja ratkaisusta kohtuullisen ajan kuluessa. (Kohta 141.)

2.4.1 Tietojen siirtäminen ja poistaminen

Tietojen siirtäminen on periaatteessa kiellettyä, paitsi rekisteröidyn niin vaatiessa tai tietyissä tapauksissa rekisterinpitäjän kuuluessa konserniin tai keskuselimeen kuuluvaan laitokseen (EU 2016/679, kohta 48). Tällaisella rekisterinpitäjällä saattaa olla oikeus siirtää henkilötietoja konsernin sisällä ilman erillistä suostumusta. Tämä koskee niin asiakkaiden kuin työntekijöiden tietoja. (EU 2016/679, kohta 48.)

Rekisterinpitäjä on myös velvoitettu lähettämään rekisteröidyn tiedot tämän toiveesta selkeästi ymmärrettävässä muodossa, sekä hänen tulee pystyä siirtämään rekisteröidyn tiedot toiseen rekisteriin tämän niin halutessa (EU 2016/679, kohta 68). Tällainen tilanne voisi Tirrosen (2018) mukaan tulla, jos kyseessä on esimerkiksi kuntosalin henkilötietorekisteri, johon on tallentunut asiakkaan sykemittaukset. Jos asiakas haluaa vaihtaa toiselle kuntosalille ja pyytää tietojaan siirrettäväksi sinne, tulisi rekisterinpitäjän toimittaa tiedot eteenpäin.

Jotkut yritykset joutuvat siirtämään asiakkaan tietoja kolmansiin maihin. Tällainen tilanne voi olla esimerkiksi matkatoimistolla. Tällöin rekisterinpitäjän vastuulla on taata, että kolmannessa maassa tietosuojan taso on EU:n komission mukaan riittävä (EU 2016/679, 45 art.).

2.5 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu tietosuoja tarkoittaa, että tietosuojan yleiset periaatteet otetaan tehokkaasti käyttöön henkilötietoja käsiteltäessä kaikissa vaiheissa (Talus ym. 2017, 13.) Käytännössä se tarkoittaa, että esimerkiksi yrityksen sisällä kaikki ovat tietoisia määrätyistä tietosuojatoimenpiteistä, eivätkä käytä tietoja väärin. Oletusarvoinen tietosuoja taas merkitsee, että rekisterinpitäjän tulee käsitellä vain erityisen tarkoituksen kannalta tarpeellisia henkilötietoja (Talus ym. 13). Tämä koskee henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Rekisterinpitäjän tulee varmistaa toimenpiteet, jotka pitävät henkilötiedot salassa rajoittamattomalta henkilömäärältä. Luonnollinen henkilö voi kuitenkin antaa suostumuksensa tietojen käyttöön myös julkisissa tilanteissa. (Talus ym. 13.)

Organisaatiossa on rekisterinpitäjän toimesta otettava käyttöön sovitut toimintaperiaatteet tietosuojan säilyttämiseen. Tämä voi tarkoittaa esimerkiksi henkilöstön koulutusta, henkilöstölle annettuja ohjeistuksia ja määräyksiä, salassapitosopimuksia, tilavalvontaa, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta, tietojen anonymisointia, tietojen pseudonymisointia, auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöönottoa. Rekisterinpitäjän tulee määritellä laajuus tietoturvan toteuttamisesta organisaatiossa riskien suuruusluokkaan perustuen. (Talus ym. 2017, 13.)

2.6 Valvontaviranomainen

Valvontaviranomainen Suomessa on tietosuojavaltuutetun toimisto. Tällä hetkellä siellä työskentelee 20 virkamiestä. (Tietosuojavaltuutetun toimisto 2018.) Näin ollen koko Suomen valvominen on haasteellista, sillä tietosuojavaltuutetun aika kuluu tutkiessa jo tulleita selvityspyyntöjä ja kysymyksiä uuteen lakiin liittyen.

2.7 Tietosuojaseloste

Tietosuoja-asetuksen (EU 2016/679) 30. artiklan mukaan jokaisen rekisterinpitäjän on pidettävä yllä kirjallista selostetta vastuullaan olevista henkilötiedoista. Sama koskee jokaista rekisterinpitäjän lukuun henkilötietoja käsittelevää tahoa. Selosteesta tulee ilmetä rekisterinpitäjän ja mahdollisen tietosuojavastaavan nimi ja yhteystiedot, käsittelyn tarkoitukset sekä kuvaus henkilötietoryhmistä, joihin rekisteröityjä kerätään. Lisäksi siitä tulee käydä ilmi henkilötietojen vastaanottajat, mikäli sellaisia on mukaan lukien tietojen siirto kolmanteen maahan tai kansainväliselle järjestölle. Myös suunnitelmat tietoryhmien mahdollisista poistoista tulee olla mainittuna. (EU 2016/679, 30 art.)

2.8 Riskien hallinta

Andreassonin ym. (2017, 30) mukaan velvoitteet ja suojatoimet tietoturvaan liittyen tulee suhteuttaa niiden aiheuttaman riskin suuruuteen. Tietojen laatua, luonnetta, käsittelytarkoitusta sekä laajuutta tulee arvioida. Riskeillä tarkoitetaan esimerkiksi sellaista tietoa, joka voi aiheuttaa rekisteröidylle fyysisiä, aineellisia tai aineettomia vahinkoja sekä johtaa syrjintään, identiteettivarkauteen, petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai arkaluontoisten tietojen paljastumiseen sivullisille. (Andreasson ym. 30.) Arkaluontoisiksi tiedoiksi voidaan luokitella esimerkiksi etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliittoon kuuluminen, geneettisiä tietoja tai terveyttä tai seksuaalista käyttäytymistä koskevat tiedot, rikostuomioita tai rikkomuksia koskevat tiedot sekä henkilökohtaiset mieltymykset ja kiinnostuksen kohteet (EU 2016/679, kohta 75). Pseudonymisoinnin paljastumisen vaara kuuluu myös arkaluontoisten tietojen listalle. Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelemistä niin, ettei rekisteröityä voida tunnistaa käyttämättä eri paikassa säilytettäviä lisätietoja. (GDPR Ready 2016.) Pseudonymisointi toimii esimerkiksi niin, että rekisteröidyn nimi on yhdessä rekisterissä numeroitu ja muualla säilytettävässä rekisterissä on numerolle annettu osoite.

Riskit ovat myös suuremmat, mitä suurempi määrä rekisteröityjä on yhdessä järjestelmässä tai kun käsitellään erityisiin henkilöryhmiin kuuluvien tai heikossa asemassa olevien tietoja, kuten lasten tietoja. Tällöin organisaatiossa tulee suorittaa vaikutustenarviointi sekä perusteellinen arvio kaikista henkilötietoihin liittyvistä riskeistä. (Andreasson ym. 2017, 30–31.)

Tirrosen (2018) mukaan riskien välttäminen ja poissulkeminen sekä pätevät tietoturvakäytännöt ovat organisaatioille merkittäviä imagon ylläpitäjiä. Uuden tietosuoja-asetuksen myötä tulevat asiakkaidenkin kriteerit nousemaan sen suhteen, millä tasolla tietosuojakäytänteet yrityksessä ovat. Jos yritys haluaa olla edelläkävijä, on tietenkin olennaista, että tällaiset lain määrittelemät seikat ovat kunnossa. Riskien puolesta myös sakottaminen tulee huomioida. (Tirronen.) Suurissa yrityksissä tietoturvarikkeestä koitunut sakko voi olla korkeimmillaan 4 % yrityksen kansainvälisestä liikevaihdosta tai 20 miljoonaa euroa (Sjöblom 2018).

Erityisiä riskiryhmiä käsittelevien rekisterinpitäjien on suoritettava vaikutustenarviointi, eli DPIA (*Data Protection Impact Assessment*) (Andreasson ym. 2017, 61). Vaikutustenarviointi koskee rekisterinpitäjiä, joilla on hallussaan henkilötietoja, jotka aiheuttavat luonnollisen henkilön kannalta korkean riskin liittyen henkilön oikeuksiin ja vapauksiin (EU 2016/679, 35 art. 1 kohta). Näitä ovat esimerkiksi terveydenhuoltoon liittyvät henkilötiedot sekä lapsia koskevat henkilötiedot. Vaikutusten arviointi on kuitenkin suotavaa joka tapauksessa, vaikkei korkean riskin tietoja kerättäisikään (VAHTI-raportti 1/2016, 21).

VAHTI-raportissa (1/2016, 21) vaikutustenarvioinnilla tarkoitetaan selvitystä, jonka perusteella pystytään hallinnoimaan riskitasoa. Riskitaso määritellään sen perusteella, kuinka suuri merkitys tietojen sisällöllä on yksilön oikeuksiin ja vapauksiin. Vaikutustenarviointi tulee suorittaa hyvissä ajoin ennen tietojen keräämistä, jotta tarvittavat hallintakeinot saadaan ajoissa käyttöön. Vaikutustenarvioinnille ei ole olemassa valmista pohjaa, sillä tietosuojauudistuksen vaatimukset vaihtelevat paljon aiheesta riippuen. (VAHTI-raportti 1/2016, 21.)

3 VIRHYDRO OY

Virhydro Oy on Virroilla sijaitseva teknisen alan myymälä, joka on perustettu vuonna 1987. Tuotevalikoimaan kuuluvat työkalut, kiinnitystarvikkeet, letkut, liittimet, työvaatteet ja -jalkineet sekä muut henkilösuojaimet, hitsausvälineet, varaosat, työkoneet, ruohonleikkurit ja paljon muuta. Virhydro Oy tarjoaa myös traktoreiden huoltopalveluja sopimuksella Agcon kanssa sekä Husqvarna-koneiden huoltopalveluja ja se on IKH-tuotteiden jälleenmyyjä. Yritykseltä löytyy verkkokauppa. Virhydro Oy:n kohderyhmään kuuluvat urakoitsijat, maa- ja metsätalousyrittäjät, teollisuusyritykset, logistiikkayritykset ja kuluttaja-asiakkaat.

Virhydro Oy on yhtiömuodoltaan osakeyhtiö, jonka on alun perin perustanut kolme osakasta. Nykyään yrityksellä on neljä osakasta ja se on hiljattain muuttunut perheyritykseksi. Toimitusjohtaja on ollut liikkeessä töissä sen perustamisvuosista lähtien ja ryhtynyt myöskin osakkaaksi ja sitä mukaa toimitusjohtajaksi jo varhaisessa vaiheessa. Virhydro Oy on kasvanut tasaisesti ikääntyessään. Toimitiloja on muokattu ja laajennettu sekä yhteistyökumppaneita ja jälleenmyyntisopimuksia on kehittynyt ajan saatossa koko ajan enemmän. Yrityksellä on ollut toimiva verkkokauppa viitisen vuotta. Yrityksellä on laaja asiakaskunta ympäri Suomen ja osa asiakaskunnasta on pitkäaikaisia liikekumppaneita. Liikevaihto on noin 3 miljoonaa euroa vuodessa.

Yrityksessä työskentelee nyt 12 henkilöä. Viisi henkilöä toimii myyjinä, kolme huollon parissa, kaksi taloushallinnossa, yksi markkinoinnissa ja yksi varastossa. Huolto-osastolla yksi työntekijöistä toimii huoltopäällikkönä ja myymälän puolella päällikkönä toimii toimitusjohtaja. (Virhydro Oy 2017.) Lisäksi liikkeessä on kesäisin vähintään kaksi kesätyöntekijää töissä.

3.1 Nykytila-analyysi

Henkilötietojen käsittelykäytänteet tulee arvioida EU:n uuden tietosuoja-asetuksen mukaisesti. Tavoitteena on, että yrityksen tuottavuus ja tehokkuus lisääntyvät tietosuojan saumattoman toimimisen kautta ja riski sanktioista ja väärinkäytöksistä saa-

daan poistettua. Virhydro Oy:n kannalta on lähdettävä tarkastelemaan henkilötietojen käsittelyä asiakasprosesseissa niin markkinoinnillisesti kuin ostotilanteessa, työntekijöiden henkilöstöhallinnossa sekä alihankkija- ja toimittajasopimuksissa. (Andreasson ym. 2017, 39.)

Virhydro Oy:lla on hallussaan pitkältä ajalta niin yksityisten henkilöiden kuin yritysten asiakastietoja lähes toista tuhatta kappaletta sekä toimittajien tietoja joitain satoja (Mäntysalmi, K. 2018). Tiedot sisältävät yritystoimintaan tarvittavat tiedot eli osoitteen, puhelinnumeron, sähköpostin sekä pankkitiedot jos kyseessä on toimittaja. Nämä ovat kaikki Futursoft-toiminnanohjausjärjestelmän muistissa. Lisäksi on olemassa nykyisten ja entisten työntekijöiden tiedot paperisena sekä vanhassa jo käytöstä poistetussa palkkaohjelmassa. Tällä hetkellä palkanlaskenta on ulkoistettu, jolloin henkilöstön tietoja välitetään palkanlaskijalle. (Mäntysalmi, T. 2018.) Myös verkkokauppa kerää asiakastietoja evästeiden avulla. Näissä kaikissa toteutuu tietojen keräämisen kannalta pätevä peruste, sillä ne ovat joko sopimuksia, suostumuksen alaisia tai niissä syntyy järkevä suhde.

Tietosuojaperiaatteet on tällä hetkellä huomioitu yrityksessä niin, että sähköiseen toiminnanohjausjärjestelmään pääsee vain omilla käyttäjätunnuksilla ja käyttäjien näkymiä pystytään muuttamaan muuttajaoikeudellisten henkilöiden käyttäjillä päällikkötasolla. Toimistoassistentin käyttäjällä on pääsy reskontrien eri osiin kuten laskutukseen, kun taas myyjien ei ole tarvetta niihin päästä kokonaisvaltaisesti. Myöskään kaikilla myyjillä ei ole pääsyä muuttamaan tai lisäämään asiakastietoja, mutta kaikki pystyvät niitä töidensä puolesta katsomaan ja niissä määrin käyttämään kuin myyntityössä tarvitsee. Lisäksi toimistoassistentin tietokone ja sähköposti, jotka sisältävät henkilöstön ja yrityksien tietoja, ovat salasanasuojattuja, niin kuin yrityksen muutkin tietokoneet. Sähköpostin välityksellä käytävä keskustelu kirjanpitäjän kanssa sisältää tietoja henkilöstön työtunneista sekä ajokilometreistä, mutta esimerkiksi lasketut palkat lähetetään salasanasuojatulla zip-tiedostolla. Palkkatietoihin ei myöskään ole pääsyä ilman erillistä salasanaa, vaikka ne onkin tallennettu tietokoneen kovalevylle. Kaikki tietokoneet on suojattu keskitetysti F-Secure virustorjuntaohjelmalla sekä palomuurilla.

Erilliset paperit koskien esimerkiksi sairaslomia, perintävaatimuksia, ammattiliittojen jäsenmaksuja tai työntekijöiden verotustietoja arkistoidaan toimistoon mappeihin.

Markkinointiviestintää tehdään tällä hetkellä pääosin sanoma- ja ammattilehdissä, mutta myös sähköpostilla ja kirjeillä lähetettävien uutiskirjeiden muodossa eri asiakasryhmille. Lisäksi internetissä tapahtuva markkinointiviestintä on merkittävää ja sitä tapahtuu Facebookin, verkkokaupan ja Instagramin välityksellä. Erilaiset markkinatapahtumat useamman kerran vuodessa kasvattavat myös asiakasvirtoja myymälään.

3.2 Riskianalyysi nykytilassa

Riskianalyysissa pohditaan Virhydron tämänhetkistä tietoturvan tasoa. Taulukosta 1 ilmenee riski, sen vakavuusaste sekä riskin toteutumisen todennäköisyys. Skenaariot on pohdittu perustuen tilanteisiin tai käytäntöihin, joihin EU:n tietosuoja-asetuksella (EU 2016/679) on vaikutusta.

Taulukko 1. Riskianalyysitaulukko.

Riskianalyysi			
Riskityyppi	**Todennäköi-syys (1-3)**	**Vakavuus (1-3)**	**Toimenpiteet**
Henkilöriskit			
Vaikeus löytää asiantuntijoita / tietoa	1	3	
Henkilöstö ei sitoudu noudattamaan annettuja ohjeita	1	3	Henkilöstö on luotettavaa.
Entiset työntekijät eivät noudata vaitiolovelvollisuutta	1	2	Heidän tietonsa vanhenevat melko pian, mutta he ovat myös luotettavia.
Henkilöstö väärinkäyttää tietoja	1	3	
Tominnalliset riskit			
Tietokoneiden hakkerointi	2	3	Virustorjunta on ajantasainen, mutta hakkerit ovat myös.
Tomistoon murtautuminen	1	2	
Mappien varastaminen	1	3	Murtautuja tuskin tietää, mitä etsiä.
Taloudelliset riskit			
Virhe tietosuoja-asetuksen soveltamisessa eli sakonuhka	1	3	Toimintasuunnitel-man laatiminen.
Markkinoinnin hankaloituminen	2	2	Asiakkaita tulee tiedottaa selkeästi.
Tietosuojavaltuutettu maksaa	1	1	Tietosuojavastaava on jo.
Vakuutuksesta aiheutuvat kulut	1	1	Vakuutusta ei oteta.
Johtamiseen liittyvät riskit			
Yhtenäisten käytäntöjen löytäminen on vaikeaa	2	2	Johdon palaverit, hekilöstön ohjeistus.
Tietosuojan valvominen on vaikeaa	1	3	
Tietosuojavastaavan kouluttaminen vie aikaa	1	3	Tietosuojavastaava on jo.
Suunnitelman toteuttaminen vie resursseja	3	3	Täytyy varautua ajoissa.
Dokumentointi on vaikeaa.	2	3	Dokumentointia varten laadittava toimintamalli.

Tiedon löytymisen riski on pieni, sillä Virhydro on valmistautunut uuteen tietosuoja-asetukseen tämän opinnäytetyön myötä. Lisäksi niin sanottu tietosuojavastaava voidaan nimetä, koska yrityksen sisältä löytyy henkilö, joka on asian tiimoilta kouluttautunut ja siihen perehtynyt. Virhydrossa virallisen tietosuojavastaavan nimeäminen ei kuitenkaan ole pakollista, sillä siellä ei käsitellä arkaluontoisia henkilötietoja tai erityisryhmiin kuuluvien henkilöiden henkilötietoja, jolloin tietosuojavastaava olisi lain velvoittama. Sjöblom (2018) ilmaisi koulutuksessaan, että uuden asetuksen myötä on suotavaa, että tietosuojavastaava on olemassa kaikissa henkilötietoja käsittelevissä yrityksissä. Henkilö kannattaa hänen mukaansa kuitenkin nimetä jollain muulla nimellä, koska viralliselle tietosuojavastaavalle saattaa tulla erilaisia lain velvoittamia tehtäviä.

Tällä hetkellä Virhydro Oy:n tietosuojauksessa on siis kohtia, joissa on riski tiedon päätymisestä vääriin käsiin. Niin halutessaan, saattaisi joku löytää vanhat palkkatietomapit toimistosta ja samalla sairaslomapaperit. Tämä voisi aiheuttaa taloudellista tai muuta syrjintää ja olla hyödynnettävää epäilyttäviin tarkoituksiin. Tietosuojauudistuksen kannalta tämä olisi tietosuojarike.

Lisäksi vedoten EU:n tietosuoja-asetuksen (EU 2016/679) 7. artiklaan tulee rekisterinpitäjän pystyä osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn. Tämä tarkoittaa, että esimerkiksi laskutusasiakassuhteen synnyttyä asiakkaan tiedot tallentuvat Futursoft-toiminnanohjausjärjestelmään sisältäen tietoja, joilla voidaan tunnistaa henkilö. Riippuen tietenkin, ovatko tiedot yrityksen vai kuluttaja-asiakkaan, niistä voi ilmetä asiakkaan puhelinnumero, sähköposti, osoite ja nimi. Tähän asti asiakastietoja on voitu hyödyntää markkinointiin lähettämällä esimerkiksi uutiskirjeitä sähköpostitse tai kirjeellä mainoskutsuja erilaisiin markkinatapahtumiin. Jos asiakas ei ole erikseen antanut suostumustaan markkinointitarkoituksiin, on se uuden lain mukaan rangaistavaa. (European Commission, [Viitattu: 29.4.2018.])

Verkkokaupassa vierailleen asiakkaan IP-osoite tallentuu järjestelmään evästeiden avulla, jolloin kuluttajakokemusta voidaan hyödyntää markkinointiin internetissä. Evästeistä on ilmoitettu nettisivuilla rekisteriselosteessa. Uuden asetuksen mukaan rekisteröitävälle tulee kuitenkin toimittaa tietojen keruuperiaatteet (EU 2016/679, 13

& 14 art.), eli tietojen saaminen tai löytäminen ei saa vaatia aktiivisuutta rekisteröitävältä (Sjöblom 2018). Evästeistä tulee siis olla ilmoitus nettisivuilla saman tien, kun käyttäjä avaa sivuston. Lisäksi evästeiden keruusta on voitava kieltäytyä ja siitä aiheutuvat seuraamukset tai sivuston toiminnan kannalta merkittävät puutteet on oltava myös heti näkyvillä. (EU 2016/679, 13 & 14 art.)

Virhydrossa ei ole tapahtunut ikinä mitään merkittäviä tietosuojavuotoja. Tietoja ei ole kukaan väärinkäyttänyt tai varastanut. Johtoportaalta kysyessäni mainittiin ainoana ulkopuolisena riskinä entiset työntekijät, joilla on ollut tiedossaan esimerkiksi asiakkaita koskevia tietoja. Riskianalyysissa on mainittu myös nykyisten työntekijöiden sitoutumattomuus, mutta sen todennäköisyys on hyvin pieni, sillä työntekijät ovat hyvin luotettavia ja lisäksi tiedot, joita he käsittelevät, eivät sisällä isoa riskiä.

4 KEHITTÄMISSUUNNITELMA

Kuviossa 1 esitetään tiivistetysti toimenpiteet, joita uuden tietosuoja-asetuksen voimaantulo yritykseltä vaatii. Se helpottaa myös selkeyttämään ajattelutapaa, mistä tietoturvan parantamisessa on kyse ja miksi toimenpiteitä tulee tehdä.

Kuvio 1. Ohjeita henkilötietojen käsittelyyn.

4.1 Tietoturvasuunnitelman esitoimenpiteet

Taulukossa 2 kuvattu aikataulu on luotu helpottamaan toimenpiteiden suunnittelua ennen tietosuoja-asetuksen siirtymäajan päättymistä Virhydrossa.

Taulukko 2. Aikataulu.

	AIKATAULU TIETOSUOJAUUDISTUKSEN TOIMENPITEILLE		
Pvm	**Tapahtuma**	**Toimenpiteet**	**Henkilöt**
21.3.-3.4.	Asiakastietolomak-keiden tekeminen	Suunnitteleminen, toteuttaminen sekä tulostaminen	Mari, Kati
6.4.	IKH-makkarapäivä	Markkinointirekiste-rin kerääminen	Mari, Tredun opiskelijoita
9.4.->	Asiakas- ja henkilöstötietojen läpikäyntiä	Vanhojen tietojen poistoa	Mari, Tuula
16.4.-15.5.	Mappien siivous	Vanhojen tietojen poistoa, lukollisen kaapin hankinta	
25.4.	Eväste-ilmoitus	Verkkokauppaan	Kati
9.4.-10.5.	Tietojen läpikäyntiä	Saatujen markkinointitieto-jen käsittelyä	Mari, Kati
11.5.	IKH-on the road-markkinapäivä	Markkinointirekiste-rin kerääminen	Mari
10.5.->	Tietojen läpikäyntiä	Saatujen asiakastietojen käsittelyä	Mari, Kati, Tuula
11.5.-24.5.	Henkilöstön ohjeistaminen		Mari
11.5.-24.5.	Markkinointirekiste-rin luominen		Mari, Kati

4.1.1 Tietojen käsittelyn tarkoitukset

Asiakastietoja tullaan keräämään asiakassuhteiden ylläpitämistä sekä tehokasta ja nopeaa kaupankäyntiä varten. Kun asiakkaalla on rekisterissä oma asiakasnumero ja sitä kautta löytyvät laskutusosoitteet ei tällaisia tietoja tarvitse vakiasiakkailta jatkuvasti kysellä ja tämä hyödyttää kaupan kumpaakin osapuolta. Myös toimittajien löytyminen rekisteristä helpottaa laskujen kirjaamista ja työ tehostuu. Lisäksi asiakastietoja halutaan hyödyntää myös markkinointiin sekä laajemman ja kattavamman myyntikokemuksen tarjoamiseen. Tämä käyttö kuitenkin vaatii erillisen luvan, koska markkinoinnilliset toimenpiteet eivät välttämättä kaikkien mielestä täytä käyttötarkoitussidonnaisuutta. Lupa siis tulee asiakkailta myös erikseen saada.

Henkilöstön tiedot kerätään työsuhteen normaalia ylläpitämistä varten.

Valvontakamerat keräävät myös dataa niin asiakkaista kuin henkilöstöstä, mutta niistä on jo olemassa ilmoitus myymälässä ja henkilöstölle kohta lisätään vielä uuteen rekisteriselosteeseen. Valvontakameroiden tarkoitus on kuitenkin olla olemassa turvallisuutta varten ja mahdollisten rikosten selvittämistä varten.

Henkilöstön tietoja säilytetään seitsemän (7) vuotta kirjanpidollisista syistä ja jos ne ovat tämän jälkeen tarpeettomia, tulee ne hävittää tai poistaa. Asiakas-, toimittaja- ja markkinointirekisterin tietojen säilyttämisaika on niin kauan, kuin yrityksen ja rekisteröidyn välillä on aktiivista toimintaa.

4.1.2 Ohjeistus henkilötietojen käsittelyyn

Tämä ohjeistus (liite 3) on tarkoitettu erityisesti henkilöstölle. Se selventää, minkä takia ja mihin perustuen sekä miten henkilötietojen käsittelyyn tulee suhtautua eri tavalla uutta asetusta noudattaen. Ohjeistus on tiivistetty muoto, jotta jokainen henkilöstön jäsen jaksaa sen myös lukea.

4.1.3 Tietojen kerääminen, poistaminen ja dokumentointi

Asiakastietoja kerätään ostotilanteissa, kun asiakas käy myymälässä tai tämän ostaessa verkkokaupasta. Jos myymälässä ilmenee, että asiakas on uusi eikä vielä näy rekisterissä, hänet kirjataan omien tietojensa perusteella asiakasrekisteriin. Samassa tilanteessa häntä pyydetään täyttämään markkinointirekisterin tietolomake (liite 4). Markkinointirekisteriä kerätään tehostetusti ennen uuden lain siirtymäajan päättymistä 25.5. Yrityksen seuraavilla markkinapäivillä 6.4. ja 11.5. tulee olemaan erillinen piste lähellä kahvipöytää, josta markkinointirekisterin tietolomakkeita löytää ja jonne ne voi täytettynä palauttaa. Tiedot on kerättävä myös vanhoilta asiakkailta uudelleen, sillä heiltä ei aikaisemmin ole kysyttyä erillistä markkinointilupaa. Markkinapäivät ovat hyvä ajankohta markkinointirekisterin keräämiselle, koska silloin myymälässä pyörii vakiasiakkaita ajan kanssa.

Asiakkaiden mielenkiinnon herättämiseksi markkinointitietolomakkeen täyttämiseen liitetään arvonta. Myöhemmin tietosuoja-asetuksen voimaantulon jälkeen markkinointirekisterin keräämislomaketta muokataan ja arvonta poistetaan, mutta asiakkailla on tietenkin mahdollisuus rekisteriin liittyä milloin vain.

Verkkokaupasta tallentuu evästeiden avulla tietoja asiakkaasta. Evästeistä tulee ponnahdusikkuna verkkokauppaan, ja tämän tekemisestä huolehtii verkkokaupan päivittäjä.

Tietojen poistaminen eri rekistereistä tapahtuu niin, että poistettavat tiedot deletoidaan toiminnanohjausjärjestelmästä. Laskuja tai sähköposteja ei kirjanpidollisista ja oikeudellisista syistä johtuen voida poistaa. Henkilöstön tiedot kuten palkkatiedot ja verotukselliset tiedot tulee kirjanpidollisista syistä säilyttää seitsemän (7) vuotta. Tämä on hyvä aika myös asiakas- ja toimittajatietojen säilyttämisen takarajaksi, mikäli ne ovat tarpeettomia. Toisinaan ilmaantuu asiakkaita tai toimittajia, jotka voivat olla toisesta maasta tai muuten vain aktivoituvat harvoin, jolloin ostojen tai myyntien välillä voi olla vuosiakin.

Henkilötietojen dokumentointia varten luodaan Excel-taulukko, johon merkataan merkittävät henkilötietoja koskevat muutokset. Exceliin voidaan esimerkiksi kirjata vuosittainen henkilötietojen tarkistuspäivä koskien niin henkilöstöä, asiakkaita kuin toimittajiakin. Tällöin pystytään käymään läpi, jos henkilöstössä on tapahtunut muutoksia tai tietoja pitää päivittää tai jos asiakas- ja toimittajarekisterissä on nimiä, jotka eivät ole suorittaneet yritykseen kohdistuvia toimintoja viimeisen seitsemän vuoden aikana. Exceliin ei merkata, kun uusi toimittaja-, asiakas- tai markkinointitieto lisätään rekisteriin, sillä niitä merkintöjä tulisi liian paljon ja työmäärä olisi kohtuuton. Sinne voidaan kuitenkin merkata muutoksista, kuten esimerkiksi päivämäärän kanssa jonkun yrityksen verkkolaskutusoperaattorin muutoksesta. Kun jonkun tiedot poistetaan seitsemän vuoden tultua täyteen tai rekisteröitävän pyynnöstä, tulee tästäkin Exceliin päivämäärällinen merkintä. Lisäksi tulevaisuudessa poistettavista tiedoista tehdään merkintä, jotta ne myös muistetaan poistaa silloin. Jotta dokumentointi ei ole vain yhden tiedoston varassa, tehdään joka vuodelle uusi taulukko ja tarpeen mukaan edellisen vuoden taulukosta siirretään päivänmääriä siihen, kuten tulevaisuudessa poistettavien tietojen merkintöjä. Näin esimerkiksi henkilöstön kohdalla tiedot eivät säily liian kauan. Asiakas- ja toimittajarekisterissä tietojen poisto

tapahtuu toiminnanohjausjärjestelmän automaattisuuden avulla. Siihen pystytään merkitsemään aika, jota vanhemmat tiedot tulee poistaa ja se poistaa ne. Näiden rekistereiden läpikäyminen tapahtuu vuosittain ja tietojen poistoa tai säilyttämistä harkitaan tapauskohtaisesti.

Taulukko 3. Esimerkki henkilötietorekisterin dokumentoinnista.

Esimerkki henkilötietojen dokumentoinnista 1.4.2018-1.4.2019			
Pvm	**Henkilö**	**Muutokset**	**Poisto**
3.4.2015	Matti Meikäläinen	Työsuhde päättynyt	3.4.2022
4.4.2018	TMI Maija Poppanen	Verkkolaskutustietoja muutettu	
5.4.2018	Anna Ainainen	Rekisteröidyn pyynnöstä tiedot poistettava asiakas- ja markkinointirekisteristä	5.4.2018
10.4.2018	Joukahainen	Lisätty henkilöstörekisteriin	
15.4.2018	asiakasnro 1234	Tiedot poistettu	

4.1.4 Tietoturvatoiminnot

Tietoturvatoimintoja lähdetään kehittämään niin, että toimistoon, jossa säilytetään muun muassa palkkatietomappeja ja muita henkilöstöön liittyviä tietoja hankitaan lukollinen kaappi, johon mapit voidaan arkistoida. Toimisto on lisäksi itsessään mahdollista lukita, mutta se ei olisi kovin toimivaa, sillä toimitusjohtajan työhuone on samassa toimistossa ja hän on lähestulkoon aina paikalla liikkeen ollessa auki. Liikkeen ulko-ovet joka tapauksessa lukitaan yöajaksi ja siellä on murtohälytysjärjestelmä ja valvontakamerat ovat toiminnassa 24/7.

Toiminnanohjausjärjestelmä huolehtii siitä, että käyttäjätunnuksilla vaihdetaan salasanat riittävän monta kertaa vuodessa.

Huhtikuussa sekä toukokuun alun aikana tulee Virhydrossa käydä henkilötietoja läpi. Vanhoja tietoja tulee hävittää koskien niin vanhoja henkilöstön tietoja kuin asiakas- ja toimittajatietoja. Asiakasrekisterissä on syytä käydä läpi päällekkäisyydet, sillä toisinaan jollekin asiakkaalle on luotu vahingossa kaksi eri asiakasnumeroa.

Myös nyt jo tiedossa olevat vanhentuneet asiakastiedot tulee poistaa koskien esimerkiksi konkurssin tehneitä yrityksiä.

Tietosuoja-assistenteiksi voidaan nimetä Mari Mäntysalmi ja Tuula Mäntysalmi, jotka tällä hetkellä vastaavat toimistoassistentin virasta.

4.1.5 Rekisteriselosteet

Rekisteriselosteet on muokattu Virhydro Oy:n aiemmasta rekisteriselosteesta. Asiakas-, markkinointi- ja toimittajarekisteriin yhdistettävä seloste (liite 1) tulee pysymään omalla paikallaan yrityksen nettisivuilla. Lisäksi uuden vaatimuksen mukaan ne tulee myös toimittaa rekisteröitäville. Näin ollen aina, kun uusi asiakas- tai toimittajasuhde syntyy, toimitetaan rekisteriseloste samalla. Asiakkaat tavataan usein myymälässä ja tällöin pyrimme saamaan heidän tietonsa kirjallisena heiltä itseltään. Samalla pystymme esittämään rekisteriselosteen. Verkkokauppa-asiakkaille seloste saadaan näkyviin rekisteröitymis- tai tilausvaiheessa.

Henkilöstörekisteriin liitettävä seloste (liite 2) toimitetaan nykyisille työntekijöille sähköpostilla ja sitä säilytetään henkilökunnan saatavilla työpaikalla. Jatkossa uusia työsuhteita solmiessa rekisteriseloste on esillä ennen työsuhteen solmimista, jotta uusi työntekijä pystyy siihen tutustumaan myös etukäteen.

YHTEENVETO

Tietosuojauudistuksen julkistamisen on voinut havaita jo kaksi vuotta sitten. Evästeilmoituksia on pystynyt lukemaan eri nettisivuilta jo vuosia ja vaatemerkkien mainoksia ei lähetetä sähköpostiin, ellei lupaa ole myönnetty. Älypuhelimien sovellukset pyytävät tietojen keräys- ja säilytyslupaa aina kun uuden sovelluksen asentaa ja some-kanavat ainakin yrittävät tarjota selosteitaan näkyville, kun kanavaan rekisteröityy.

Tietosuojan pyrkimys on turvata jokaisen oikeudet omien tietojensa puolesta ja tämä tulee toki muistaa myös itse kuluttajana. Yrityksen kannalta uudistus tuntuu työläältä projektilta, joka vaatii paljon aiheeseen perehtymistä sekä käytäntöjen muuttamista. Yritystoiminnassa ei kuitenkaan riitä, että vain yksi henkilö on aiheesta tietoinen, vaan se tulee saattaa myös muun henkilöstön tietoon ja myös tämä aiheuttaa paljon työtä. Virhydrossa asetuksen sisäistäminen onnistuu sen kokoluokan puolesta vielä melko helposti, mutta suuret organisaatiot ovat varmasti joutuneet palkkaamaan erityisiä ammattilaisia perehtymään aiheeseen ja ohjeistamaan muita. Koulutustilaisuuksissa tavattuani muita yrityksien edustajia olivat asetuksen radikaaleimmat muutokset ihmetyksen kohteena, etenkin tietojen käytön laillisuusperiaatteet. Erityistä hankaluutta on myös opinnäytetyötä tehdessäni aiheuttanut suoramarkkinointiin suhtautuminen. Siihen on tulkintoja yhtä paljon kuin on tulkintojen antajiakin. Joidenkin mielestä se saadaan upotettua asetuksen vaatimuksiin ja toisten mielestä taas ei. Itse olen tulkinnut, että asiakastietojen käyttö suoramarkkinointiin ei ole laillista ja sen takia olen luonut markkinointirekisterin ja jatkan sillä, kunnes joitain muita mahdollisuuksia yritykselle ilmenee.

Suomen hallituksen suunnittelema tietosuojalaki olisi varmasti vähän asetusta selventävä laki, mutta sen ollessa vielä eduskunnan käsittelyssä, ei siitä ole hyötyä tietosuoja-asetukseen varautuessa. Tampereen koulutuksessa todettiin, että esityksen piti mennä eduskuntaan jo syksyllä 2017. Reipas myöhästyminen on aiheuttanut sen, että lakia ei ole vieläkään saatu voimaan. Myös tietosuojavaltuutetun toimisto antaa täsmennyksiä artikloihin, mutta siellä ollaan niin ylityöllistettyjä, että laajoja ohjeistuksia ei nopealla aikavälillä voi odottaa.

Opinnäytetyöni pohjalta toimenpiteet ovat kohdeyrityksessä lähteneet hyvin käyntiin. Koen tämän olleen aiheena äärimmäisen hyvä, sillä kohdeyrityksessä ollaan oltu hyvin tyytyväisiä annettuihin ohjeisiin. Aiheena tietosuojauudistus on ollut hyvin opettavainen ja vaatinut asioiden miettimistä monella eri tapaa. Työn merkitys on myös ollut Virhydrolle suuri.

Uskon, että tietosuojavaltuutetun toimesta sekä ylipäätään käytännössä jotkin tulkinnat asetuksen kohdista tulevat ajan kanssa vakiintumaan, mutta aluksi se voi synnyttää ristiriitoja. Monelle kuluttajalle tietosuojauudistus on täysin uusi asia ja itsekin olen saanut monta kertaa sen tarkoitusta asiakkaalle selittää. Yritykset ovat asiasta melko tietoisia, jolloin heidän yhteyshenkilönsä myös ymmärtävät tilanteen. Luulen kuitenkin, että sen suurempaa haittaa tietosuojauudistuksesta ei yrityksen toiminnalle synny. Vanhojen tietojen poistaminen on varmasti joka tapauksessa hyväksi ja lisäksi se vapauttaa hylly- ja mappitilaa.

LÄHTEET

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma.

D 95/46/EY. Henkilötietodirektiivi.

EU 2016/679, 4.5.2016. Euroopan parlamentin ja neuvoston asetus. Euroopan unionin virallinen lehti L 119/1. [Verkkojulkaisu.] [Viitattu: 24.4.2018] Saatavana: http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=FI

Euroopan unionin perusoikeuskirja. 26.10.2012. Euroopan unionin virallinen lehti. C 326/391. [Verkkojulkaisu.] [Viitattu: 2.4.2018] Saatavana: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A12012P%2FTXT

European Commission. [Verkkosivu]. [Viitattu: 29.4.2018]. Saatavana: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_en

GDPR Ready 2018. 2016. [Verkkosivu]. [Viitattu: 12.2.2018]. Saatavana: http://www.gdpr.fi/

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017 Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

L 22.4.1999/523. Henkilötietolaki.

Mäntysalmi, K. 2018. Toimitusjohtaja. Henkilökohtainen tiedonanto. Virhydro Oy.

Mäntysalmi, T. 2018. Toimistoassistentti. Henkilökohtainen tiedonanto. Virhydro Oy.

Regulation of the European Parliament and of the Council (EU) 2016/679, 4.5.2016. The Official Journal of the European Union. [Verkkojulkaisu.] [Viitattu: 29.4.2018] Saatavana: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

Sjöblom, S. 14.3.2018 Yritysakatemia: Tietosuojasääntelyn uudistus. Koulutus. Tampere.

Talus, A., Autio, E., Hänninen, A., Pihamaa H-T. & Kantonen, S., 27.1.2017. Miten valmistautua EU:n tietosuoja-asetukseen? 4/2017. [Verkkojulkaisu]. Helsinki: Oikeusministeriö & Tietosuojavaltuutetun toimisto. [Viitattu: 29.4.2018]. Saatavana: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojalait 2016. Lakikokoelmat. Helsinki: Edita.

Tietosuojavaltuutetun toimisto 2018. [Verkkosivu.] [Viitattu: 24.4.2018] Saatavana: http://www.tietosuoja.fi/fi/

Tirronen, U. 15.2.2018 Hallintoakatemia: EU:n tietosuoja-asetus ja henkilötietojen käsittely. Koulutus. Virrat.

VAHTI-raportti 1/2016. [Verkkojulkaisu.] [Viitattu: 4.3.2018] Saatavana: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Virhydro Oy. 2017. [Verkkosivu]. [Viitattu 9.2.2018]. Saatavana: www.virhydro.fi

Yrittäjän tietosuojaopas. 2018. Suomen Yrittäjät ry. [Verkkosivu]. [Viitattu: 28.2.2018]. Saatavana: https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018.pdf

LIITTEET

Liite 1. Rekisteriseloste henkilöstörekisteriin

Liite 2. Rekisteriseloste markkinointi-, asiakas- ja toimittajarekisteriin

Liite 3. Henkilöstön ohjeistus

Liite 4. Markkinointirekisterilomake

LIITE 1 Rekisteriseloste hekilöstörekisteriin

Tämä rekisteriseloste on henkilöstöä varten ja se julkaistaan työsopimuksen teon yhteydessä sekä säilytetään henkilöstön saatavilla.

1. Rekisteriseloste

Euroopan parlamentin ja neuvoston asetus, 2016.

Laatimispäivä 8.3.2018

2. Rekisterinpitäjä

Virhydro Oy

Pirkantie 22, 34800 Virrat

FINLAND

010 2711 200

3. Rekisteriasioista vastaava

Tuula Mäntysalmi / Virhydro Oy

y-tunnus: 0654232-9

Pirkantie 22, 34800 Virrat

FINLAND

etunimi.sukunimi@virhydro.fi

4. Rekisterin nimi

Virhydro Oy:n henkilöstörekisteri

5. Henkilötietojen käsittelyn tarkoitus (rekisterin käyttötarkoitus)

Tietoja käsitellään työsuhteen ylläpitämiseen tarvittaviin toimenpiteisiin.

6. Rekisterin tietosisältö

Rekisteri sisältää rekisteröityjen nimet, osoitteet, henkilötunnukset, sähköpostit, puhelinnumerot, pankkitiedot sekä verotukselliset tiedot.

7. Säännönmukaiset tietolähteet

Työsopimuksen allekirjoitusvaiheessa rekisteröity hyväksyy tietojensa tarpeelliseen käsittelyyn sekä luovuttaa tiedot tarpeen mukaan. Muita tietolähteitä ovat ulosottovirasto, työterveyshuolto sekä koulutustahot.

8. Säännönmukaiset tietojen luovutukset

Tietoja luovutetaan palkanlaskijalle, verottajalle ja ulosottovirastolle, eläke- ja tapaturmavakuutusyhtiöille, työterveyshuollolle sekä koulutustahoille.

9. Tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle

Ei tietojen luovutuksia EU:n tai ETA:n ulkopuolelle.

10. Rekisterin suojauksen periaatteet

Paperisia tietoja säilytetään mapeissa lukollisessa tilassa / kaapissa. Tietokoneella käsiteltävät tiedot on suojattu palomuurilla ja virustorjunnalla, toiminnanohjausjärjestelmä omilla käyttäjätunnuksilla sekä pääsyjen rajoittamisella, palkkatiedot on salasanasuojatussa tiedostossa myös palkanlaskijalle lähetettäessä.

11. Rekisteröidyn tarkastusoikeus

Rekisteröidyllä on oikeus tarkastaa rekisteriin tallennetut itseään koskevat tiedot ja saada niistä kopiot. Tarkastuspyyntö tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilölle.

12. Tiedon korjaaminen

Rekisterinpitäjä oikaisee, poistaa tai täydentää rekisterissä olevan, käsittelyn tarkoituksen kannalta virheellisen, tarpeettoman, puutteellisen tai vanhentuneen henkilötiedon oma-aloitteisesti tai rekisteröidyn vaatimuksesta. Rekisteröidyn tulee ottaa yhteyttä rekisterinpitäjän rekisteriasioista vastaavaan henkilöön tiedon korjaamiseksi.

13. Tietojen säilyttäminen

Henkilöstön tietoja säilytetään työsuhteen päätyttyä seitsemän (7) vuotta, paitsi jos lainmukainen tarve tai tietojen luovuttaminen esimerkiksi verottajalle vaatii myöhempää tiedossa olevaa käsittelyä.

14. Kameravalvonta

Myymälässä on tallentava kameravalvonta ja tallenteita saatetaan hyödyntää tarpeen vaatiessa esimerkiksi rikostutkintaan.

LIITE 2 Rekisteriseloste markkinointi-, asiakas- ja toimittajarekisteriin

Tässä rekisteriselosteessa on käsitelty markkinointi-, asiakas- ja toimittajarekisteri koskien niin fyysisiä asiakkaita kuin verkkokauppa-asiakkaita. Rekisteriseloste julkaistaan Virhydro Oy:n verkkosivuilla.

1. Rekisteriseloste

Euroopan parlamentin ja neuvoston asetus, 2016.

Laatimispäivä 8.3.2018

2. Rekisterinpitäjä

Virhydro Oy

Pirkantie 22, 34800 Virrat

FINLAND

010 2711 200

3. Rekisteriasioista vastaava

Tuula Mäntysalmi / Virhydro Oy

Virhydro Oy

y-tunnus: 0654232-9

Pirkantie 22, 34800 Virrat

FINLAND

etunimi.sukunimi@virhydro.fi

4. Rekisterin nimi

Virhydro Oy:n asiakas- / toimittajarekisteri

5. Henkilötietojen käsittelyn tarkoitus (rekisterin käyttötarkoitus)

Virhydro Oy:n verkkokaupan käyttäjärekisteriin tallennettuja henkilötietoja käytetään asiakassuhteiden hoitamiseen, yhteydenottojen hoitamiseksi, luvallisiin markkinointitarkoituksiin sekä muihin verkkopalveluihin liittyviin tarkoituksiin.

Asiakasrekisteriin tallennetaan laskutusasiakkaiden tiedot. Tietoja käsitellään laskutus- ja myyntitilanteissa.

Toimittajarekisteriin tallennetaan toimittajien tiedot. Tietoja käsitellään ostotilanteissa sekä laskujen maksamisessa.

6. Rekisterin tietosisältö

Rekisteriin kerätään asiakkaan tai toimittajan (henkilö tai yritys) nimi, osoite, mahdollinen y-tunnus, puhelinnumero sekä sähköposti. Toimittajatiedoissa on lisäksi pankkitiedot.

7. Säännönmukaiset tietolähteet

Rekisterinpitäjä rekisteröi Virhydro Oy:n verkkokaupan käyttäjästä ne tiedot, jotka käyttäjä itse ilmoittaa verkkosivustoa käyttäessään.

Myymäläasiakkailta tiedot saadaan rekisteröitävältä itseltään kuten toimittajiltakin.

8. Säännönmukaiset tietojen luovutukset ja tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle

Ei säännönmukaisia tietojen luovutuksia kolmansille osapuolille. Ei tietojen luovutuksia EU:n tai ETA:n ulkopuolelle.

9. Rekisterin suojauksen periaatteet

Virhydro Oy:n verkkokaupan käyttäjärekisterin tiedot on tallennettu rekisterinpitäjän järjestelmään. Järjestelmään sisäänpääsy edellyttää käyttäjätunnuksen ja salasanan syöttämistä. Järjestelmä on myös suojattu palomuurein ja muiden teknisten keinojen avulla. Järjestelmään tallennettuihin rekisterin sisältämiin tietoihin pääsevät ja

niitä ovat oikeutettuja käyttämään vain tietyt, ennalta määritellyt rekisterinpitäjän työntekijät. Rekisterin sisältämät tiedot sijaitsevat lukituissa ja vartioiduissa tiloissa.

10. Rekisteröidyn kielto-oikeus

Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten. Kielto tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilöille.

11. Rekisteröidyn tarkastus-oikeus

Rekisteröidyllä on oikeus tarkastaa rekisteriin tallennetut itseään koskevat tiedot ja saada niistä kopiot. Tarkastuspyyntö tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilölle.

12. Tiedon korjaaminen

Rekisterinpitäjä oikaisee, poistaa tai täydentää rekisterissä olevan, käsittelyn tarkoituksen kannalta virheellisen, tarpeettoman, puutteellisen tai vanhentuneen henkilötiedon oma-aloitteisesti tai rekisteröidyn vaatimuksesta. Rekisteröidyn tulee ottaa yhteyttä rekisterinpitäjän rekisteriasioista vastaavaan henkilöön tiedon korjaamiseksi.

13. Evästeiden käyttö verkkokaupassa

Virhydro Oy verkkokauppa käyttää evästeitä käyttäjäkokemuksen parantamiseksi.

Eväste (cookie) on pieni tekstitiedosto, joka tallennetaan tilapäisesti käyttäjän kiintolevylle. Evästeitä käytetään lähes kaikilla verkkosivustoilla, eivätkä sivustot välttämättä toimi kunnolla ilman evästeitä.

Eväste sisältää satunnaisesti luodun yksilöivän tunnuksen, jonka avulla voimme tunnistaa laitteesi ja kerätä tietoa siitä, mitä sivuja ja toimintoja verkkokaupassa käytät.

14. Evästeet ja tilastointi

Käytämme Google Analytics -ohjelmaa kerätäksemme tietoja siitä, miten verkkokauppaa käytetään. Tietojen avulla pyrimme saamaan käsityksen siitä, mitä verkkokaupan asiakkaat haluavat ja miten voimme parhaiten antaa asiakkaille hyvän käyttökokemuksen.

15. Evästeiden estäminen ja poistaminen

Voit estää evästeiden käytön laitteellasi muuttamalla selaimesi asetuksia. Asetusten sijainti riippuu selaimesta. Kannattaa kuitenkin ottaa huomioon, että monet toiminnot edellyttävät, että verkkokauppa tallentaa tekemäsi valinnat. Jos estät evästeet, et välttämättä voi käyttää kaikkia toimintoja.

16. Tietojen säilyttäminen

Asiakas- ja toimittajatietoja säilytetään rekisterissä niin kauan, kuin asiakkaan tai toimittajan ja yrityksen välillä on aktiivista toimintaa.

LIITE 3 Ohjeistus henkilöstölle

Ohjeistus henkilöstölle

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4.5.2016

EU:n uutta tietosuoja-asetusta aletaan soveltamaan lainsäädäntöön 25.5.2018 alkaen. Uuden tietosuoja-asetuksen tavoitteena on parantaa henkilötietojen suojaa ja rekisteröityjen oikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa sekä edistää digitaalisten sisämarkkinoiden kehittymistä.

Uusi tietosuoja-asetus korvaa henkilötietodirektiivin (95/46/EY) sekä Suomen henkilötietolain (523/1999).

Henkilötiedoilla tarkoitetaan tietojen perusteella tunnistettavaan henkilöön liittyviä tietoja. Näitä ovat esimerkiksi nimi, osoite, henkilötunnus, puhelinnumero, sähköposti tai sijaintitiedot, jotka saattavat liittyä myös yrityskontakteihin tai työntekijätietoihin. Henkilötietorekisteri on mikä tahansa henkilötietoja sisältävä lista kuten asiakasrekisteri.

Tämä ohjeistus on laadittu Virhydro Oy:n tietosuoja-assistentin Mari Mäntysalmen toimesta. Kysymykset liittyen tietosuoja-asioihin voi esittää Tuula Mäntysalmelle (etunimi.sukunimi@virhydro.fi) tai Mari Mäntysalmelle (etunimi.sukunimi@virhydro.fi).

1. Tietojen käsittelyn tulee olla laillista; siihen tulee olla suostumus tai sopimus (alle 16-v huoltajan), oikeutettu etu (ts. asiakkuus), lakisääteinen velvoite tai elintärkeä tai yleinen etu.
2. Tietoturvaloukkauksista sekä merkittävistä tietosuojamuutoksista, kuten poistoista tai tietojen antamisesta rekisteröidylle, tulee tehdä ilmoitus tietosuoja-assistentille dokumentaatiota varten.
3. Pääsääntöisesti tietoja ei saa luovuttaa kolmansille osapuolille.
4. Rekisteröidyllä on oikeus saada tietoonsa hänestä säilytettävät tiedot, korjauttaa virheelliset tiedot sekä tulla unohdetuksi.
5. Yleisten tietosuojaperiaatteiden mukaan tietojen ja niiden käsittelyn tulee olla lainmukaista, kohtuullista ja läpinäkyvää, niistä tulee käydä ilmi käyttötarkoitussidonnaisuus eikä tietoja tulisi kerätä tai säilyttää ylimääräistä tai turhaan. Tietojen tulee myös olla täsmällisiä, eheitä ja luottamuksellisia.
6. Uuden tietosuoja-asetuksen nojalla henkilötietorekistereitä ylläpitäviä yrityksiä, yhdistyksiä tai organisaatioita voidaan rangaista sakon uhalla väärinkäytöksistä.

LIITE 4 Markkinointirekisterilomake

LIITY VIRHYDRON MARKKINOINTIREKISTERIIN JA OSALLISTU ARVONTAAN

Liity Virhydron markkinointirekisteriin täyttämällä tämä lomake. **21.5.2018 mennessä rekisteriin liittyneiden kesken arvotaan Bahcon työkalusarja (arvo 159€)**. Rekisterin jäsenille voidaan lähettää markkinointiviestejä ajankohtaisista tarjouksista sekä kutsuja tapahtumiin. Tietoja ei luovuteta kolmansille osapuolille.

EU:n uutta tietosuoja-asetusta aletaan soveltamaan lainsäädäntöön 25.5.2018 alkaen. Uuden tietosuoja-asetuksen tavoitteena on parantaa henkilötietojen suojaa ja rekisteröityjen oikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa sekä edistää digitaalisten sisämarkkinoiden kehittymistä. Tietosuoja-asetus edellyttää asiakkaan suostumusta suoramarkkinointiin.

Nimi:

Yritys:

Toimitusosoite:

Sähköposti:

Puhelinnumero:

◯ Tehkää merkintä tähän, mikäli haluatte osallistua vain arvontaan.