Juha Keinänen

Valmistautuminen EU:n yleiseen tietosuoja-asetukseen

Tradenomi

Tietojenkäsittely

Kevät 2018

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä(t): Keinänen Juha

Työn nimi: Valmistautuminen EU:n yleiseen tietosuoja-asetukseen

Tutkintonimike: Tradenomi, Tietojenkäsittely

Asiasanat: EU:n yleinen tietosuoja-asetus, tietosuoja, tietoturva, henkilötieto, henkilötietojen käsittely, rekisterinpitäjä

Opinnäytetyön tilaajana toimi Koillis-Suomen kehittämisyhtiö Naturpolis Oy. Yhtiö toimii Kuusamon ja Taivalkosken alueilla ja sen tehtävänä on edistää näillä alueilla yritysten toimintaedellytyksiä ja toimintaympäristöä, uusien työpaikkojen syntymistä ja alueellista elinkeinoyhteistyötä.

Opinnäytetyön tavoitteena oli perehtyä EU:n yleiseen tietosuoja-asetukseen ja avustaa Naturpolis Oy:tä valmistautumaan tietosuoja-asetuksen mukanaan tuomiin vaatimuksiin. Opinnäytetyö toteutettiin kehittämistyönä, jonka tavoitteena oli perehtyä Naturpolis Oy:n toimintaan tietosuoja-asetuksen vaatimusten kannalta ja tuottaa ohjeistuksia tietosuoja-asetuksen eri vaatimusten täyttämiseksi.

Teoriaosuus aloitettiin perehtymällä opinnäytetyöhön liittyviin peruskäsitteisiin, kuten tietosuoja, tietoturva ja henkilötietojen käsittely. Nämä käsitteet ovat olennainen osa EU:n tietosuoja-asetusta, joten niihin perehtyminen oli hyvä lähtökohta työn toteuttamiselle. Teoriaosuus jatkui tietosuoja-asetuksen olennaisen sisällön esittelyllä. Päätavoitteena oli käydä tietosuoja-asetuksen sisältöä läpi ja löytää sieltä vaatimukset, jotka pitää tulevaisuudessa huomioida Naturpolis Oy:n toiminnassa.

Opinnäytetyön tuloksena syntyi joukko suosituksia ja ohjeistuksia tietosuoja-asetuksen vaatimuksiin liittyen. Lisäksi tämän opinnäytetyön sisältöä ja tietosuoja-asetukseen liittyviä vaatimuksia esitellään Naturpolis Oy:n henkilökunnalle tietosuoja-asetukseen liittyvässä kokoustilaisuudessa.

Abstract

Author(s): Keinänen Juha

Title of the Publication: Preparing for General Data Protection Regulation

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: General Data Protection Regulation (GDPR), data protection, information security, personal data, processing of personal data, data controller

This thesis was commissioned by Naturpolis Oy which is a business development company that operates in Kuusamo and Taivalkoski region. Its task is to develop and promote operational preconditions and environment for businesses, the creation of new jobs and regional business cooperation.

The purpose of this thesis was to study the GDPR and help Naturpolis Oy prepare for the upcoming requirements of the GDPR. The thesis was done as a development work. The goal was to get acquainted with Naturpolis Oy's activities, compare the activities with GDPR requirements and develop instructions for meeting the requirements.

The theoretical part began with studying and introducing some basic concepts related to the thesis, such as data protection, information security and processing of personal data. These concepts are highly relevant to the GDPR so studying and introducing them was a good starting point for the thesis. After that the theoretical part continues with the introduction of the GDPR itself. Main goal was to study the content of GDPR and find all the requirements that would be relevant for Naturpolis Oy in future.

The result of the thesis was a group of recommendations and instructions regarding the requirements of GDPR. The content of this thesis and requirements of GDPR will also be introduced to the staff of Naturpolis Oy in a GDPR-related meeting at a later date.

Sisällys

1 Johdanto

Henkilötietojen käsittelyn määrä ja merkitys nyky-yhteiskunnassa kasvaa jatkuvasti. Etenkin Internetissä liiketoimintaa harjoittavat yritykset tuottavat usein palveluita, joiden toiminnassa henkilötietojen käsittely on avainasemassa. Esimerkiksi verkkokaupat kysyvät asiakkailtaan tietoja, joiden avulla tilatut tuotteet toimitetaan perille. Tämän lisäksi on yleistä, että verkkokaupat keräävät taustalla muutakin tietoa, jonka avulla esimerkiksi kohdennetaan tietynlaisia tarjouksia tietyille käyttäjille. Ehkä vielä parempana esimerkkinä ovat sosiaaliset mediat, jotka yleensä ovat käyttäjilleen enimmäkseen ilmaisia käyttää ja niiden liiketoiminta perustuukin mainontaan ja tietojen keräämiseen.

Henkilötietojen käsittely onkin niin olennainen osa arkipäiväisiä toimintoja, että se tapahtuu ison osan ajasta huomaamattamme. Moni käyttäjä ei esimerkiksi välttämättä tiedosta, että rekisteröityessään vaikka uuteen sosiaaliseen mediaan kysytään häneltä lupaa tiettyjen tietojensa käyttämiseen esimerkiksi markkinointia varten. Tällöin voikin herätä kysymyksiä henkilötietojen käsittelyn ja keräämisen eettisyydestä tai laillisuudesta.

Euroopan unionin maissa ihmisillä on laeissa säädetty oikeus tietosuojaan. Vaikka lainsäädäntö voi poiketa maasta riippuen, on tietosuojalakien päätavoitteena yleisesti turvata ihmisten oikeus yksityisyyteen. Henkilötietojen käsittelystä on säädetty Suomessa Henkilötietolaissa 523/1999 ja EU:n tasolla aiemmin tietosuojadirektiivissä 95/46/EC. Direktiiviä 95/46/EC ei kuitenkaan ole koettu riittäväksi ja EU-alueella on aiemmin ollut 28 erilaista tietosuojalakia käytössä. Lainsäädännön harmonisaatio onkin yksi isoimmista syistä, miksi EU-alueella aletaan pian soveltamaan EU:n yleistä tietosuoja-asetusta.

EU:n yleinen tietosuoja-asetus (General Data Protection Regulation) annettiin 27.4.2016 ja sitä aletaan soveltamaan noin kahden vuoden siirtymäajan jälkeen 25.5.2018 alkaen. Se koskee kaikkia EEA-alueella (EEA-alueeseen kuuluvat EU:n jäsenmaat, Norja, Islanti ja Liechtenstein) toimivia organisaatioita ja sen tavoitteena on muun muassa yhtenäistää EU:n tietosuojalainsäädäntöä ja parantaa yksilöiden oikeuksia. Samalla se tuo organisaatioille uusia velvoitteita, joihin tulee valmistautua siirtymäajan puitteissa.

Opinnäytetyön tilaajana on Kuusamon ja Taivalkosken alueilla toimiva Koillis-Suomen kehittämisyhtiö Naturpolis Oy. Yhtiö toimii Kuusamon ja Taivalkosken alueilla ja sen yhtiön tehtävänä on edistää näiden kuntien alueilla yritysten toimintaedellytyksiä ja toimintaympäristöä, uusien työpaikkojen syntymistä ja alueellista elinkeinoyhteistyötä.

Opinnäytetyön tavoitteena on tutustua EU:n yleisen tietosuoja-asetuksen vaatimuksiin ja auttaa Naturpolis Oy:tä valmistautumaan niihin. Opinnäytetyössä lähdetään liikkeelle teoriaosuudella, jossa aluksi perehdytään aiheeseen liittyviin peruskäsitteisiin ja tämän jälkeen EU:n yleisen tietosuoja-asetuksen sisältöön. Käytännön osuudessa tutustutaan Naturpolis Oy:n toimintaan ja tarkastellaan sitä tietosuoja-asetuksen vaatimusten näkökulmasta. Tavoitteena käytännön osuudessa on antaa suosituksia ja luoda ohjeistuksia, jotta tietosuoja-asetuksen vaatimukset voidaan täyttää Naturpolis Oy:ssä.

2 Henkilötietojen käsittely

Vuosina 1988 ja 1989 Suomessa tuli vaiheittain voimaan henkilörekisterilaki ja henkilörekisteriasetus. Henkilörekisterilaki oli ensimmäinen henkilötietojen käsittelyyn liittyvä yleislaki Suomessa. Seuraavien vuosien aikana siihen tehtiin muutamia muutoksia, kunnes se kumottiin henkilötietolailla vuonna 1999. (Vanto 2011, 17.)

Henkilötietolain tarkoituksena on lain ensimmäisen pykälän mukaan ”toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista”. Lakia sovelletaan tiettyjä poikkeustilanteita lukuun ottamatta aina henkilötietoja käsiteltäessä. Poikkeustilanteita voivat olla muun muassa luonnollisen henkilön henkilökohtaisiin, yksityisiin tarkoituksiinsa suorittamaa henkilötietojen käsittelyä. (L 523/1999, 1§.)

Henkilötietolaissa noudatetaan pitkälti samanlaisia periaatteita kuin tulevassa tietosuoja-asetuksessakin. Tällaisia periaatteita ovat muun muassa tietojen keräämisen ja käsittelyn läpinäkyvyys, asianmukaisuus, käyttötarkoitussidonnaisuus ja turvallisuus. Tietosuojan tulee olla aina olla mukana käsittelyn joka vaiheessa. Rekistereistä on laadittava rekisteriselosteet, joista ilmenee rekisterin käyttötarkoitus, kuvaus sisällöstä, kuvaus tietovirroista ja kuvaus suojauksen periaatteista. Rekisteröidyillä on oikeus saada tietoa käsittelystä, tarkastella omia tietojaan, oikaista virheellisiä tietoja ja kieltää tietojensa käsittelyä suoramainontaa ja etämyyntiä varten. (L 523/1999, 26§; Tietosuojavaltuutetun toimisto 2010.)

Tulevan EU:n yleisen tietosuoja-asetuksen perusperiaatteet ovat hyvin samankaltaisia kuin nykyisen henkilötietolain periaatteet. Tietosuoja-asetuksessa täsmennetään jonkin verran tiettyjä käsitteitä, mutta niiden idea pysyy samana. Yksi keskeisimpiä muutoksia on osoitusvelvollisuuden korostuminen. Henkilötietolain aikana on riittänyt, että säännöksiä noudatetaan, mutta tietosuoja-asetuksen myötä organisaatioilla tulee olla keinot myös osoittaa, että säännöksiä noudatetaan. Tämä onkin yksi isoimmista tietosuoja-asetuksen tuomista haasteista organisaatioille, joilla ei ole vielä keinoja osoitusvelvollisuuden täyttämiseksi. Osoitusvelvollisuuden täyttäminen vaatiikin uudenlaista lähestymistapaa tietosuojan toteuttamiselle. (Talus, Autio, Hänninen, Pihamaa, Kantonen & tietosuojavaltuutetun toimisto 2017, 14)

Henkilötietojen käsittelytoimintaan liittyy monia käsitteitä, joiden tunteminen on tärkeää henkilötietojen oikeanlaisen käsittelyn toteuttamisen ja lainsäädännön ymmärtämisen kannalta. Tässä luvussa käydään läpi aiheen keskeisimpiä käsitteitä.

Henkilötieto

Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevalla henkilöllä tarkoitetaan tässä tapauksessa luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa henkilötietojen avulla. (A 2016/679, artikla 4.) Perushenkilötieto voi olla esimerkiksi henkilötunnus, joka voidaan suoraan tunnistaa tietyn henkilön henkilötiedoksi. Koska käsitteeseen sisältyy kaikki suoraan tai epäsuorasti henkilöön liittyvä tieto, lasketaan henkilötiedoiksi yllättävän kuuloisiakin tietoja. Tällaisia tietoja voivat olla muun muassa IP-osoite, evästetiedostot tai verkkoselaimen selaushistoria. Onkin tärkeää, että käsitteen laajuus ymmärretään suunniteltaessa esimerkiksi liiketoimintaan liittyviä asioita. (Vanto 2011, 22.)

Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan toimintaa, jota kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Käsittelyksi lasketaan tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla saataville, yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen. (A 2016/679, artikla 4.) On huomioitava, että henkilötietojen käsittelijä ei välttämättä ole rekisterinpitäjä. Henkilötietojen käsittelijä ei ole rekisterinpitäjä, jos se ei pysty määräämään henkilötietojen käyttötarkoitusta tai keinoja. (Vanto 2011, 31.)

Rekisteri

Rekisterillä tarkoitetaan ”mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu” (A 2016/679, artikla 4.)

Rekisterinpitäjä

Rekisterinpitäjä on ”luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”. (A 2016/679, artikla 4.) Keskeisenä asiana rekisterinpitäjällä on oikeus määrätä rekisterin käyttötarkoituksesta ja keinoista. (Vanto 2011, 22.)

Tietoturva

Tietoturvalla tarkoitetaan kaikkia toimenpiteitä, joilla pyritään suojaamaan rekisteröityjen yksityisyyttä, oikeuksia ja vapauksia. (Suomen tietosuojapalvelut Oy n.d. Periaatteet, politiikat ja suunnitelmat.) Perinteisesti tietoturvan keskeiset tavoitteet on jaettu kolmeen osaan:

- Luottamuksellisuus
- Eheys
- Käytettävyys.

Näiden lisäksi tavoitteita voivat myös olla seuraavat:

- Kiistämättömyys
- Todentaminen.

Luottamuksellisuuden turvaamisella pyritään siihen, että vain asianmukaiset henkilöt pääsevät näkemään vain heille tarkoitettua tietoa. Eheyden varmistamisella pyritään säilyttämään tiedon alkuperäinen muoto ja estämään tiedon muuttaminen ilman asianmukaisia valtuutuksia. Tiedon saatavuudella pyritään siihen, että tieto on aina saatavilla, kun sitä tarvitaan. Kiistämättömyydellä tarkoitetaan sitä, että tietojärjestelmien toimintaa seurataan niin, että käyttäjät eivät voi kiistää tekojaan toimiessaan tietojen kanssa. Todentamisella tarkoitetaan tapoja, joilla käyttäjät pystyvät esimerkiksi käyttäjätunnusten ja salasanojen avulla todentamaan heidän henkilöllisyytensä. (Laakso n.d.)

Tietoturvan kolmen keskeisen tavoitteen toteuttaminen on haastavaa. Esimerkiksi luottamuksellisuuden toteuttaminen voi helposti olla ristiriidassa saatavuuden kanssa, jos tieto turvataan niin tehokkaasti, että vahingossa asianmukaisiltakin henkilöiltä evätään

pääsy siihen. Siksi onkin tärkeää, että tietoturvan toteutus suunnitellaan huolellisesti niin, että jokainen osa-alue toteutuu mahdollisimman tehokkaasti. (Laakso n.d.)

Tietosuoja

Tietosuojalla käsitteenä tarkoitetaan rekisteröidyn tietoihin liittyvien oikeuksien, yksityisyyden ja luottamuksen turvaamista. Tietosuojan tavoitteena on taata henkilötietojen oikeanlainen käsittely ja estää niiden luvaton käsittely. Suomessa tietosuoja on käytännössä nykyisen henkilötietolain vaatimusten täyttämistä niin, että rekisteröityjen oikeudet toteutuvat. (Suomen tietosuojapalvelut Oy n.d. Tietosuoja.)

Tietoturvaloukkaus

Tietoturvaloukkauksella tarkoitetaan tapausta, jossa tieto tahattomasti tai tahallisesti tuhoutuu, katoaa tai muuttuu. Lisäksi tietoturvaloukkaus voi olla tapaus, jossa tietoja joutuu vääriin käsiin tai tietoihin päästään luvattomasti käsiksi. (Suomen Yrittäjät 2018.) Tietoturvaloukkaus voi ilmetä monenlaisissa muodoissa, kuten esimerkiksi kyberhyökkäyksenä, varastettuna kovalevynä, tuhoutuneena tietokoneena tai jo ainoastaan puhumalla äänekkäästi arkaluontoisista tiedoista väärässä seurassa. Loukkausten seuraamukset riippuvat muun muassa loukkauksen kohteena olevan tiedon luonteesta ja määrästä. (Tietosuojavaltuutetun toimisto 2017a.)

Tietoturvaloukkaukset on pyrittävä estämään suojaamalla henkilötiedot mahdollisimman hyvin. Suojaustoimenpiteiden tulee vastata tietoihin kohdistuvan riskin tasoa. Tietoturvaloukkauksia ei kuitenkaan voi täydellä varmuudella estää aina tapahtumasta. Tämän takia on varauduttava tietoturvaloukkausten tapahtumiseenkin mahdollisimman hyvin. Pohdittavia asioita ovat muun muassa vahinkojen minimoiminen, loukkausten analyysi ja dokumentointi, vastaavien loukkausten estäminen tulevaisuudessa ja tietoturvaloukkauksen mahdollinen ilmoittaminen valvontaviranomaiselle ja loukkauksen uhrille. (Tietosuojavaltuutetun toimisto 2017a.)

Tietotilinpäätös

Tietotilinpäätöksellä tarkoitetaan organisaation tietovarantoihin, tietojohtamiseen, tietojenkäsittelyyn ja tietoturvallisuuteen kohdistuvaa tilinpäätösraporttia. Sille on olemassa monenlaisia toteuttamistapoja, jotka voivat vaihdella organisaation laajuudesta, luon-

teesta ja toiminnasta riippuen. Sen tehtävänä on kuitenkin yleensä antaa kokonaiskuva organisaation tietojenkäsittelystä. Tietotilinpäätöksen avulla voidaan saavuttaa parempi ymmärrys organisaation tietojenkäsittelytoiminnasta, jolloin mahdollisia ongelmakohtia voidaan ratkoa ja täten parantaa organisaation toimintaa. Lisäksi tietotilinpäätöksen tekeminen edesauttaa tietosuoja-asetuksen osoitusvelvollisuuden täyttämistä. (Tietosuojavaltuutetun toimisto 2010.)

Tietotilinpäätöksessä voidaan kuvailla esimerkiksi

- organisaation tietovarannot
- tietoarkkitehtuuri
- tietojen laatu ja käytettävyys
- menettelytavat ja periaatteet henkilötietojen käsittelyssä
- miten tiedot on suojattu ja miten tietojen käsittelyä valvotaan
- miten rekisteröityjen oikeudet toteutetaan
- arviointi mahdollisista toiminnan kehittämismahdollisuuksista. (Tietosuojavaltuutetun toimisto 2010.)

Riskienhallinta

Riskienhallinnalla tarkoitetaan riskeihin kohdistuvia toimenpiteitä. Riskienhallinta voi koostua esimerkiksi seuraavista asioista:

1. Toimintaympäristön määrittely
2. Riskien tunnistaminen
3. Riskianalyysi
4. Riskien merkitysten arviointi
5. Riskien käsittely
6. Seuranta.

Riskienhallinta lähtee liikkeelle toimintaympäristön määrittelystä. Henkilötietojen käsittelyn kannalta riskienhallinta kohdistuu henkilötietoihin. Kohdat 2–3 muodostavat riskien arviointiprosessin. Tässä prosessissa pyritään ottamaan selville, mitä riskejä on olemassa, miten todennäköisesti ne ilmenevät ja miten merkittäviä niiden vaikutukset ovat. Riskien suuruus määräytyy näiden mukaan. Arvioinnin jälkeen riskien ehkäisemiseksi voidaan tarpeen mukaan kehitellä erilaisia keinoja ja panna ne käytäntöön. Lopuksi seurataan, että onko riskienhallinta onnistunut ja tarpeen mukaan riskienhallintaprosessi tehdään uudelleen. (Rousku 2017.)

Riskienhallintaan on olemassa työkaluja. Esimerkiksi EU:n yleisen tietosuoja-asetuksen myötä JUHTA-yhteishanke on kehittänyt Excelissä toimivan riskienhallintatyökalun, jota yritykset voivat käyttää apunaan. (Valtiovarainministeriö 2018.)

Johtava valvontaviranomainen

EU:n yleisessä tietosuoja-asetuksessa puhutaan johtavan valvontaviranomaisen roolista. Tämä valvontaviranomainen on vastuussa henkilötietojen käsittelyn valvomisesta, jos organisaatio toimii useammassa maassa tai jos henkilötietojen käsittelyn kohteena on useamman kuin yhden EU:n jäsenvaltion kansalaisia. Pääasiallisesti johtava valvontaviranomainen on organisaatiolle sen maan valvontaviranomainen, jossa organisaation päätoimipaikka sijaitsee. (Tietosuojavaltuutetun toimisto 2017b.)

Suomessa henkilötietolaissa on määritelty tietosuojaviranomaisista. Tällä hetkellä Suomen johtavana valvontaviranomaisena toimii tietosuojavaltuutettu. (L 523/1999, 38–41§.) Jos organisaation tarvitsee toimittaa tietosuojaan tai henkilötietojen käsittelyyn liittyviä selvityksiä tai muita ilmoituksia, tulee organisaation olla siis yhteydessä tietosuojavaltuutettuun ja toimittaa tarvittavat selvitykset tietosuojavaltuutetun toimistolle.

3 EU:n yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus astui voimaan 24. toukokuuta 2016 ja sitä aletaan soveltamaan 25. toukokuuta 2018 alkaen. Siirtymäajan aikana organisaatioiden on varmistettava, että henkilötietojen käsittely organisaatiossa tapahtuu tietosuoja-asetuksessa määriteltyjen vaatimusten mukaisesti. (Talus ym. 2017, 13–14.)

Tietosuoja-asetuksen sisältö koskee sekä EEA-alueella toimivia organisaatioita että EEA-alueen kansalaisten tietoja käsitteleviä organisaatioita. (Karjalainen 2018.) Asetus koskee sekä yksityisen että julkisen sektorin toimijoita riippumatta henkilötietojen käsittelyn laajuudesta tai luonteesta. (Talus ym. 2017, 9.)

3.1 Syitä uudelle lainsäädännölle

Tietosuoja-asetuksella pyritään harmonisoimaan EU-alueen tietosuojalainsäädäntöä. Ennen tietosuoja-asetusta EU-alueella oli voimassa 28 erilaista tietosuojalakia. Uuden asetuksen tarkoituksena on yhdenmukaistaa tietosuojalainsäädäntö yhden asetuksen alle. (Karjalainen 2018.)

Tietosuoja-asetuksen myötä henkilötietojen käsittely muuttuu avoimemmaksi ja läpinäkyvämmäksi. Rekisteröidyillä henkilöillä on paljon laajemmat mahdollisuudet saada tietoa siitä, mitä tietoja hänestä kerätään, mihin tarkoitukseen, miten niitä käsitellään ja kenelle ne voivat joutua. Rekisterinpitäjille ja henkilötietojen käsittelijöille tulee uusia velvoitteita, joiden mukaan heidän täytyy laatia muun muassa julkisia selosteita henkilötietojen käsittelystä. (Talus ym. 2017, 9.)

Harmonisoidun lainsäädännön ja avoimuuden tuoman luottamuksen kasvun myötä tietosuoja-asetuksen toivotaan parantavan digitaalitalouden kehitystä sisämarkkinoiden ja EU-kumppanien alueella. (Ala-Varvi 2017.)

3.2 Henkilötietojen käsittelyä koskevat periaatteet

Tietosuoja-asetuksessa määritellään joukko periaatteita, joita rekisterinpitäjän tulee noudattaa henkilötietojen käsittelyssä. Nämä periaatteet ovat

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- osoitusvelvollisuus.

Näitä periaatteita on noudatettava henkilötietojen kaikissa käsittelyvaiheessa. Lisäksi tietosuoja-asetuksessa korostuu osoitusvelvollisuus, jonka myötä rekisterinpitäjän on kyettävä todistamaan, että periaatteita noudatetaan. (A 2016/679, 5 artikla.)

3.3 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksessa määritellään sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet. Sisäänrakennetulla tietosuojalla tarkoitetaan, että aikaisemmin mainitut tietosuojaperiaatteet huomioidaan tarkasti henkilötietojen käsittelyn jokaisessa vaiheessa suunnittelusta soveltamiseen. (Talus ym. 2017, 13–14.) Oletusarvoisella tietosuojalla tarkoitetaan, että oletusarvoisesti jokaisessa henkilötietojen käsittelyn vaiheessa käsitellään vain käsittelyn kannalta olennaisia henkilötietoja. Oleellisia kriteerejä tätä pohtiessa ovat käsittelyn laajuus sekä henkilötietojen määrä, elinkaari ja saatavuus. Oletusarvoisen tietosuojan toteuttamisessa on etenkin huomioitava se, että oletusarvoisesti henkilötiedot eivät ole rajoittamattoman henkilömäärän saatavissa ilman luonnollisen henkilön myötävaikutusta. (Talus ym. 2017, 13–14.)

Kun toteutetaan asianmukaisia teknisiä ja organisatorisia toimenpiteitä tietosuoja-asetuksen siirtymäaikana, on huolehdittava sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden toteutumisesta toimenpiteissä. (Talus ym. 2017, 13–14.)

3.4 Osoitusvelvollisuus

Ennen tietosuoja-asetusta on yleensä riittänyt, että tietosuojaan liittyviä säännöksiä ja periaatteita noudatetaan. Tietosuoja-asetuksen myötä organisaatioilla on myös osoitusvelvollisuus. Tämä tarkoittaa sitä, että säännösten ja periaatteiden noudattaminen on kyettävä osoittamaan tarvittaessa. (Talus ym. 2017, 14.)

Pääasiassa osoitusvelvollisuus voidaan täyttää huolellisella dokumentoinnilla, josta käy ilmi tietosuoja-asetuksen vaatimusten täyttämiseksi tehdyt toimenpiteet, prosessit ja säännöstelyt. Pääsääntöisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden on ylläpidettävä selostetta, josta käy ilmi vastuuna olevat käsittelytoimet. Selosteessa tulee kuvailla muun muassa

- rekisterinpitäjän ja tietosuojavastaavan yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- kenelle henkilötietoja luovutetaan
- henkilötietojen elinkaari
- mahdollisuuksien mukaan yleinen kuvaus teknisistä ja organisatorisista turvatoimista.

Tämä seloste tulee olla kirjallisena ja sellaisessa muodossa, että sen voi toimittaa pyydettäessä viranomaiselle. (A 2016/679, 30 artikla.)

3.5 Riskiperusteinen lähestymistapa

Tietosuoja-asetuksessa sovelletaan riskiperusteista lähestymistapaa. Tämä tarkoittaa sitä, että organisaation velvoitteet ja vaadittavat toimenpiteet henkilötietojen suojaamiselle suhteutetaan rekisteröityjen oikeuksille kohdistuvaan riskiin. Tämän lähestymistavan tavoitteena on pyrkiä välttämään ylisääntelyä etenkin sellaisissa tilanteissa, joissa henkilötietoihin kohdistuva riski on matala. (Talus ym. 2017, 16.)

Jotta riskiperusteista lähestymistapaa voidaan soveltaa, tarvitaan henkilötietojen käsittelytoimista riskikartoitus. Riskikartoituksessa pyritään selvittämään muun muassa käsitel-

tävien tietojen luonne, tietojen määrä, mahdolliset vahingot seuraamukset tietovuodon sattuessa ja mahdollisuudet vuodon sattumiselle. Riskit kasvavat sitä mukaa kuin mitä enemmän tietoja käsitellään ja mitä arkaluontoisempaa tietoa käsitellään. Lisäksi riskin tasoa nostavat mahdolliset vahingot, palautumisaika ja riskin toteutumisen mahdollisuus. (Talus ym. 2017, 16.)

3.6 Henkilötietojen käsittelyperusteet

Tietosuoja-asetuksen mukaan henkilötietojen käsittelyn tarve on pystyttävä perustelemaan. Asetuksessa määritellään joukko edellytyksiä, joista vähintään yhden tulee täyttyä, jotta käsittelyllä on pätevä oikeusperusta. Nämä edellytykset ovat seuraavat:

- Käsittely on tarpeellista sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi.
- Rekisteröity on antanut vapaaehtoisesti suostumuksen käsittelylle. Alle 16-vuotiaiden tapauksessa vaaditaan huoltajan suostumus. Jäsenvaltiot voivat säätää omassa lainsäädännössään tätä ikärajaa alemmaksi 13 ikävuoteen asti.
- Käsittely on tarpeellista rekisterinpitäjän tai kolmannen osapuolen etujen toteuttamiselle, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja –vapaudet syrjäyttävät tällaiset edut.
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.
- Käsittely on tarpeen yleisen edun kannalta.
- Käsittely on tarpeen elintärkeiden etujen suojaamisen kannalta. (Karjalainen 2018.)

3.7 Rekisteröidyn oikeudet

Tietosuoja-asetuksessa määritellään rekisteröidylle erilaisia oikeuksia tämän henkilötietojen ja niiden käsittelyn suhteen. Rekisterinpitäjällä on velvollisuus toteuttaa näitä oikeuksia ja organisaatioissa onkin tehtävä suunnitelma näiden velvollisuuksien noudattamiseksi. (Talus ym. 2017, 23.)

Oikeus saada tietoa henkilötietojen käsittelystä

Tietosuoja-asetuksessa korostetaan, että rekisterinpitäjällä on velvollisuus tiedottaa avoimesti henkilötietojen käsittelystä. Rekisteröidyille henkilöille on tiedotettava muun muassa seuraavanlaisia henkilötietojen käsittelyä koskevia tietoja:

- Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot
- Syyt henkilötietojen käsittelylle ja käsittelyn oikeusperusta
- Kenelle tietoja mahdollisesti luovutetaan eteenpäin
- Henkilötietojen säilytysaika ja perustelut säilytysajan pituudelle
- Tiedotus rekisteröidyn oikeuksista
- Tiedotus oikeudesta valittaa valvontaviranomaiselle
- Henkilötietojen luovuttamisen pakollisuus ja seuraamukset, jos rekisteröity ei suostu luovuttamaan tietoja
- Selvitys mahdollisesta automaattisesta päätöksenteosta ja profiloinnista.

Jos rekisterinpitäjä kerää rekisteröidystä henkilötietoja muista lähteistä kuin suoraan rekisteröidyltä, tulee rekisterinpitäjän ilmoittaa myös

- kerättävät tiedot
- henkilötietojen lähde
- selvitys siitä, että onko lähde yleisesti saatavilla.

Näistä asioista koostuva seloste on oltava julkisesti saatavilla ja sen ajantasaisuudesta tulee huolehtia. (Valtiovarainministeriö 2016, 14.)

Oikeus päästä käsiksi tietoihin

Tietosuoja-asetuksessa määritellään rekisteröidyille oikeus saada pääsy kaikkiin omiin henkilötietoihinsa rekisterissä. Jos rekisteröity tekee tällaisen pyynnön, on siihen reagoitava pääsääntöisesti yhden kuukauden aikana. Määräaikaa voidaan jatkaa tarvittaessa kahdella kuukaudella. Määräajan nostamisen perusteina voi olla pyyntöjen monimutkai-

suus ja määrä. Määräajan nostamisesta on kuitenkin ilmoitettava kuukauden sisällä rekisteröidylle ja samalla kerrottava viivästyksen syyt. (Talus ym. 2017, 24–25.)

Jos pyynnön lähettäjän henkilöllisyydestä on epäilystä ja epäilys on perusteltu, rekisterinpitäjä voi vaatia lähettäjää toimittamaan lisätietoja henkilöllisyyden varmistamiseksi. Onkin tärkeää, että rekisteröidyn henkilöllisyydestä ei ole epäilystä tietoja luovutettaessa, koska tässä tapauksessa vaarana on tietojen päätyminen vääriin käsiin. Rekisteröity voi pyytää tietojen lähettämistä sähköisesti, jolloin tiedot on lähetettävä yleisesti luettavassa sähköisessä muodossa. Pyynnöt on lähtökohtaisesti toteutettava maksuttomasti, mutta tietyin edellytyksin niistä voi pyytää hallinnollisista kustannuksista aiheutuvat kulut. Rekisterinpitäjä voi myös kieltäytyä toimen suorittamisesta, jos rekisteröidyn pyynnöt ovat ilmeisen kohtuuttomia tai perusteettomia. Tällaisessa tapauksessa rekisterinpitäjällä on tosin osoitusvelvollisuus kohtuuttomuudesta tai perusteettomuudesta. (Talus ym. 2017, 24–25.)

Oikeus tietojen oikaisemiseen ja ”oikeus tulla unohdetuksi”

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää korjaamaan virheellisiä tietoja tai täydentämään puutteellisia tietoja. (A 2016/679, 16 artikla.)

Rekisteröidyllä on myös ”oikeus tulla unohdetuksi”, eli hän voi tietyin ehdoin pyytää rekisterinpitäjää poistamaan häntä koskevat henkilötiedot ilman aiheetonta viivytystä. Tätä oikeutta ei voida soveltaa, jos on kyse lakisääteisistä rekistereistä. Oikeutta voidaan soveltaa muun muassa seuraavien ehtojen täyttyessä:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne alun perin kerättiin.
- Rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut.
- Rekisteröity käyttää vastustamisoikeuttaan ja käsittelyyn ei ole olemassa perusteltua syytä.
- Henkilötietojen käsittely on ollut lainvastaista.
- Henkilötiedot on poistettava rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi. (A 2016/679, 17 artikla.)

Oikeus siirtää tietoja järjestelmästä toiseen

Rekisteröidyllä on oikeus saada siirrettyä henkilötietojaan järjestelmien välillä. Tätä varten henkilö voi pyytää rekisterinpitäjältä henkilötietojaan sellaisessa muodossa, että ne voidaan siirtää toiselle rekisterinpitäjälle. Tiedot voidaan siirtää myös suoraan rekisterinpitäjältä toiselle, jos tämä on teknisesti mahdollista. Siirto-oikeus ei velvoita rekisterinpitäjiä suunnittelemaan tai toteuttamaan järjestelmiä niin, että ne ovat yhteensopivia keskenään. Siirto-oikeus tuo kuitenkin pohdittavaksi sen, että miten tiedot kerätään ja luovutetaan mahdollisimman vähin vaivoin. (Valtiovarainministeriö 2016, 16)

Oikeus siirtoon on vain, jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen ja jos käsittely suoritetaan automaattisesti. Organisaatioissa on selvitettävä, että koskeeko siirto-oikeus organisaatiossa käsiteltäviä henkilötietoryhmiä. (Talus ym. 2017, 26–27.)

Oikeus rajoittaa käsittelyä

Rekisteröidyllä on oikeus vaatia, että häneen liittyvien tietojen käsittelyä rajoitetaan. Kun käsittelyä on rajoitettu, tietoja saa säilytyksen lisäksi käyttää muutamaa poikkeustilannetta lukuun ottamatta vain rekisteröidyn suostumuksella. (Talus ym. 2017, 26.)

Oikeus käsittelyn rajoittamiselle on, jos

- tietojen paikkansapitävyys kyseenalaistetaan rekisteröidyn toimesta
- käsittely on lainvastaista ja rekisteröity vaatii tietojen poistamisen sijaan tietojen käytön rajoittamista
- rekisterinpitäjä ei enää tarvitse henkilötietoja, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- rekisteröity on käyttänyt vastustamisoikeuttaan. Käsittelyä rajoitetaan niin kauan kun kestää todentaa, että syrjäyttävätkö rekisterinpitäjän perusteet rekisteröidyn perusteet käsittelylle.

Jos käsittelyä on rajoitettu, rekisterinpitäjän on tiedotettava rekisteröidylle ennen kuin rajoitus poistetaan. (Talus ym. 2017, 26.)

Oikeus vastustaa käsittelyä

Rekisteröidyllä voi olla tietyissä tilanteissa oikeus vastustaa hänen tietoihin kohdistuvaa käsittelyä. Rekisteröidyn käyttäessä vastustamisoikeutta rekisterinpitäjän on lähtökohtaisesti keskeytettävä tämän rekisteröidyn henkilötietojen käsittely. Poikkeuksena on tilanteet, jossa käsittelyyn on huomattavan tärkeä ja perusteltu syy, joka menee rekisteröidyn oikeuksien edelle tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Talus ym. 2017, 27.)

Suoramarkkinointia koskevissa tapauksissa vastustamisoikeutta voidaan käyttää, jos rekisteröity haluaa estää tietojensa käytön suoramarkkinoinnissa. Samoin voi toimia myös tieteellisten, historiallisten tai tilastollisten tutkimusten suhteen, mutta näihin voi olla erilaisia poikkeustilanteita, joista on säädetty kansallisessa laissa. (Talus ym. 2017, 27.)

Vastustamisoikeudesta on tiedotettava rekisteröidylle selkeästi ja muusta tiedotuksesta erillään viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran. (Talus ym. 2017, 27.)

Oikeus vastustaa automaattista päätöksentekoa ja profilointia

Tiettyjä poikkeustilanteita lukuun ottamatta tietosuoja-asetus kieltää sellaisten automatisoituun käsittelyyn perustuvien päätösten tekemisen, joilla on rekisteröityjä koskevia oikeusvaikutuksia tai jotka vaikuttavat rekisteröityyn vastaavalla tavalla merkittävästi. Poikkeustilanteita ovat seuraavat:

- Päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten.
- Päätös on hyväksytty rekisterinpitäjään sovellettavassa unionin tai jäsenvaltion lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi.
- Päätös perustuu rekisteröidyn suostumukseen. (Valtiovarainministeriö 2016, 16.)

3.8 Henkilötietojen käsittelyn ulkoistaminen, sopimukset ja tarjouspyynnöt

Rekisterinpitäjä voi myös ulkoistaa henkilötietoihin käsittelyyn liittyviä tehtäviä. Ulkoistettuna palveluna voidaan pitää esimerkiksi henkilötietojen säilytyskapasiteetin ostamista. Kun henkilötietojen käsittelyä ulkoistetaan, tulee henkilötietojen käsittelijän taata, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Tietosuoja-asetuksen noudattamista voidaan osoittaa noudattamalla hyväksyttyjä käytännesääntöjä tai sertifiointimekanismeja. Nykyiset sopimukset on syytä käydä läpi siirtymäajan puitteissa. (Talus ym. 2017, 22.)

Tietosuoja-asetuksen mukaan rekisterinpitäjän ja ulkoisen henkilötietojen käsittelijän on sovittava tietyistä seikoista toimeksiantosopimuksessa. Näitä asioita ovat

- henkilötietojen käsittelyn kohde, luonne, tarkoitus, tyyppi, kesto ja rekisteröityjen ryhmät
- rekisterinpitäjän velvollisuudet ja oikeudet
- sopimus siitä, että henkilötietojen käsittelijä saa käsitellä tietoja ainoastaan rekisterinpitäjän ohjeistusten mukaisesti
- varmistus siitä, että henkilötietoja käsittelevillä henkilöillä on salassapitovelvollisuus
- sopimus siitä, että käsittelyä ei ulkoisteta toiselle käsittelijälle ilman kirjallista lupaa rekisterinpitäjältä
- sopimus tietoturvaloukkausten ilmoittamiseen liittyvien velvollisuuksien noudattamisesta
- sopimus osoitusvelvollisuuden toteuttamiseksi tarvittavien tietojen luovuttamisesta rekisterinpitäjälle
- salliminen rekisterinpitäjän tekemille auditoinneille
- sopimus palvelun päättymisen yhteydessä tapahtuvasta henkilötietojen palauttamisesta tai poistamisesta. (Hämäläinen 2017.)

Tietosuoja-asetuksen vaatimukset on huomioitava sekä nykyisissä että uusissa sopimuksissa. Tarjouspyynnöissä tietosuoja-asetuksen vaatimusten toteutuminen pitäisi myös ottaa huomioon. Tarjouspyynnössä kannattaa huomioida ainakin

- tietojen sijainti, liikkuvuus ja näihin liittyvät lainsäädännölliset asiat
- palvelun tietosuojaan ja tietoturvallisuuteen liittyvien vaatimusten määrittely
- tietosuoja-asetuksen noudattamiseksi tarvittavat yhteistyöasiat, kuten ilmoitusvelvollisuudet, raportointi ja vastuuasiat
- salassapito ja muut sitoumukset. (Hämäläinen 2017.)

EU-US Privacy Shield

EU-US Privacy Shield on Yhdysvaltain kauppaministeriön, Euroopan komission ja Sveitsin hallinnon suunnittelema järjestely, jonka tarkoituksena on turvata EU-kansalaisten perusoikeuksia silloin, kun kansalaisten henkilötietoja siirretään Yhdysvaltoihin. Järjestelyyn voivat liittyä mukaan sekä yhdysvaltalaiset ja eurooppalaiset organisaatiot. Jotta järjestelyyn voi liittyä mukaan, tulee organisaation todistaa Yhdysvaltain kauppaministeriölle, että järjestelyssä määriteltyjä sääntöjä noudatetaan organisaatiossa. Lisäksi organisaation tulee julkisesti sitoutua sääntöjen noudattamiseen. On tärkeää huomioida, että Privacy Shield -järjestely ei ole osana tietosuoja-asetusta, vaan se on EU:n ja Yhdysvaltain välinen sopimus ja keino, jolla organisaatiot voivat osoittaa noudattavansa tietosuoja-asetuksen periaatteita. (US Department of Commerce 2018b.)

Privacy Shield -järjestelyn avulla pyritään saamaan EU-kansalaisille samat perusoikeudet myös silloin, kun henkilötietojen käsittely siirtyy Yhdysvaltoihin. Privacy Shieldin tarkoituksena on muun muassa estää sen puitteissa käsiteltäviin henkilötietoihin kohdistuva laajamittainen massavalvonta (Kansallisen tiedusteluviraston johtaja täsmentää, että tietoja voitaisiin kerätä vain tiukoin ehdoin) ja antaa EU-kansalaisille oikeussuojakeinoja ja riidanratkaisumenetelmiä. (US Department of Commerce 2018b.)

Privacy Shield -järjestelyyn kuuluu yli 2900 organisaatiota, joihin lukeutuu merkittäviä yhtiöitä, kuten Google, Microsoft ja Facebook. (US Department of Commerce 2018a.)

3.9 Tietoturvaloukkausten kanssa toimiminen

Rekisterinpitäjän on ilmoitettava henkilötietoihin kohdistuvasta tietoturvaloukkauksesta sekä valvontaviranomaiselle että rekisteröidyille, joiden henkilötietoihin tietoturvaloukkaus on kohdistunut. Ilmoitus on jätettävä valvontaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta lähtien ja rekisteröidylle ilman aiheetonta viivytystä. Jos ilmoitusta ole annettu valvontaviranomaiselle 72 tunnin kuluessa, on valvontaviranomaiselle toimitettava perusteltu selitys. Jos taas rekisteröidylle ei ole ilmoitettu loukkauksesta, voi valvontaviranomainen joko vaatia ilmoituksen tekemistä tai päättää tietyin ehdoin, että ilmoitusta ei tarvitse tehdä. Tällaisia ehtoja ovat seuraavat:

- Rekisterinpitäjä on toteuttanut asianmukaiset suojatoimenpiteet (esimerkiksi salaus), joiden avulla loukkauksen kohteena olleet henkilötiedot eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa tietoihin.

- Rekisterinpitäjä on jatkotoimenpiteillä varmistanut, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu.

- Ilmoitus vaatisi kohtuutonta vaivaa. Esimerkiksi yksittäiset tiedotukset laajassa loukkaustapauksessa vaativat paljon organisaatiolta ja tällaisessa tapauksessa esimerkiksi julkinen tiedonanto onkin suositeltavaa. (A 2016/679, 33–34 artiklat.)

Jos tietoturvaloukkauksen havaitsee henkilötietojen käsittelijä, on tämän ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä. (A 2016/679, 33–34 artiklat.)

Ilmoituksen voi jättää tekemättä kokonaan, jos tietoturvaloukkaus ei todennäköisesti aiheuta riskiä luonnollisten henkilöiden oikeuksille ja vapauksille. (A 2016/679, 33–34 artiklat.)

Valvontaviranomaiselle tehtävässä ilmoituksessa on käytävä ilmi vähintään seuraavat asiat:

- Kuvaus tietoturvaloukkauksesta, asianomaisten rekisteröityjen ryhmistä ja arvioiduista lukumääristä sekä henkilötietotyyppien ryhmistä ja arvioiduista lukumääristä.

- Tietosuojavastaavan nimi, yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa.

- Kuvaus tietoturvaloukkauksen todennäköisistä seurauksista.

- Kuvaus rekisterinpitäjän ehdottamista ja toteutetuista toimenpiteistä, jotka on suoritettu tietoturvaloukkauksen johdosta.

- Kuvaus mahdollisista toimenpiteistä haittavaikutusten lieventämiseksi. (A 2016/679, 33–34 artiklat.)

Rekisteröidylle tehtävässä ilmoituksessa on käytävä ilmi samat asiat ensimmäistä kohtaa lukuun ottamatta. (A 2016/679, 33–34 artiklat.)

Kaikki tietoturvaloukkaukset on dokumentoitava niin, että dokumentoinnista käy ilmi tietoturvaloukkausten luonne, vaikutukset ja toteutettavat korjaustoimenpiteet. Dokumentoinnin avulla valvontaviranomainen voi tarkistaa, että rekisterinpitäjä noudattaa ilmoitusvelvollisuuttaan. (A 2016/679, 33–34 artiklat.)

Organisaatioissa tulisi suunnitella käytännöt tietoturvaloukkauksia varten. Pohdittavia asioita ovat tietoturvaloukkausten tunnistamistavat, ilmoittamiset, selvitykset ja dokumentointi. Jotta ilmoitusvelvollisuutta voidaan noudattaa, tarvitaan valmiita suunnitelmia ja ohjeistusta organisaation sisällä näiden suunnitelmien toteuttamista varten. (Talus ym. 2017, 32–33.)

3.10 Tietosuojavastaavan määrittämisen tarve

Jos organisaatio toimii rekisterinpitäjänä tai henkilötietojen käsittelijänä, voi tietosuoja-asetus vaatia, että organisaatioon nimitetään tietosuojavastaava. Tietosuojavastaavan tehtäviin kuuluvat mm. huolehtiminen henkilötietojen käsittelyn lainmukaisuudesta, tietosuoja-asioihin liittyvä neuvonta ja tietosuojaan liittyvien tiedustelujen yhteyspisteenä toimiminen. Tietosuojavastaava toimii ensimmäisenä yhteyspisteenä, kun toimitaan valvontaviranomaisen kanssa. (A 2016/679, 37–39 artiklat.)

Tietosuojavastaava on nimitettävä aina, jos

- organisaatio on julkisen sektorin toimija, joka ei ole tuomioistuin

- organisaation henkilötietojen käsittelyyn liittyvät ydintehtävät muodostuvat laajamittaisesta, säännöllisestä ja järjestelmällisestä seurannasta

- organisaation ydintehtävät muodostuvat erityisiin tietoryhmiin, rikostuomioihin tai rikoksiin liittyvästä henkilötietojen käsittelystä. (A 2016/679, 37–39 artiklat.)

Jos nämä ehdot eivät täyty, voi tietosuojavastaavan nimittää myös vapaaehtoisesti halutessaan. Onkin syytä pohtia, että olisiko tietosuojavastaavan nimittämisestä hyötyä organisaation toiminnalle. Vastaavaa ei kuitenkaan kannata nimittää turhaan, koska vapaaehtoisesti nimetyllä vastaavalle on samat velvollisuudet ja tämä saattaa aiheuttaa turhaa vaivaa organisaatiolle. (Mäkelä 2018.)

Vaikkei tietosuojavastaavaa nimitetä, kannattaa tietosuojasta huolehtiminen kuitenkin vastuuttaa jollekin henkilölle tai ryhmälle, joka huolehtii muun muassa dokumentoinnista. (Karjalainen 2018.)

Tietosuojavastaavan asema on riippumaton. Vastaava ei saa vastaanottaa ohjeita tehtävän suorittamisessa ja hän raportoi suoraan ylimmälle johdolle. Nimitettäessä tietosuojavastaavaa tulee huomioida ehdokkaan pätevyys rooliin. Vastaavalla tulee olla ammattipätevyyttä sekä asiantuntemusta tietosuojalainsäädännöstä ja alan käytänteistä. Rooliin voi nimittää joko organisaation henkilöstön jäsenen tai palvelusopimuksen perusteella toimivan henkilön. Tällä henkilöllä saa olla organisaatiossa muitakin tehtäviä, kunhan ne eivät ole ristiriidassa tietosuojavastaavan asemaan liittyvien tehtävien kanssa. (A 2016/679, 37–39 artiklat.)

3.11 Seuraamukset laiminlyönnistä

Jos rekisterinpitäjä tai henkilötietojen käsittelijä laiminlyö tietosuoja-asetuksessa määriteltyjä velvoitteita, valvontaviranomainen voi määrätä erilaisia seuraamuksia laiminlyöjälle. Näitä seuraamuksia ovat hallinnolliset sakot, varoitus, huomautus, määräys tai käsittelykielto. Seuraamukset ovat samantasoisia kaikissa EU:n kaikissa jäsenvaltioissa. (JUHTA 2017.)

Hallinnollisen sakon suuruus voi olla maksimissaan joko 4 prosenttia vuosivaihdosta tai 20 miljoonaa euroa (riippuen siitä, kumpi on isompi summa). Sakon summa määräytyy rikkomuksen mukaan tapauskohtaisesti ja maksimisakkoon vaaditaankin huomattavan vahingollinen rikkomus. (A 2016/679, 83 artikla.)

3.12 Tietosuoja-asetuksen tulkinta

Kun tietosuoja-asetus astui voimaan vuonna 2016, asetukseen liittyvät käytännön asiat eivät vielä olleet täysin selviä. Siirtymäajan kuluessa EU:n tietosuojaryhmä WP 29 on laatinut erilaisia ohjeistuksia tietosuoja-asetuksen tulkintaan liittyen. Näitä ohjeistuksia julkaistaan ryhmän verkkosivuilla ja tietosuoja-asetuksen tulkintaa varten suositellaankin tutustumaan niihin. Tulkinta kuitenkin tarkentuu entisestään vasta oikeuskäytännön kautta. Lisäksi tietosuoja-asetus jättää jäsenmaiden lainsäädäntöön liikkumavaraa, joten lainsäädännön kehittämistä kannattaa seurata myös siirtymäajan loppumisen jälkeenkin tarkasti. (Talus ym. 2017, 36–37.)

4 Koillis-Suomen Kehittämisyhtiö Naturpolis Oy

Työn tilaajana toimii Koillis-Suomen kehittämisyhtiö Naturpolis Oy. Yhtiö on vuonna 2005 perustettu Kuusamon kaupungin ja Taivalkosken kunnan omistama elinkeinojen kehittämisyhtiö. Yhtiön tehtävänä on edistää Kuusamon ja Taivalkosken alueilla yritysten toimintaedellytyksiä ja toimintaympäristöä, uusien työpaikkojen syntymistä ja alueellista elinkeinoyhteistyötä. Yhtiö tekee aluemarkkinointia sekä yritys- ja aluekehitystä hanketoiminnan kautta. (Naturpolis Oy 2018.)

Naturpolis Oy tarjoaa palveluja sekä uusille että toiminnassa oleville yritykselle. Tarjottavia palveluja ovat mm. perusneuvonta, rahoitusneuvonta, laskelmat, kehittämissopimukset ja asiantuntijaverkoston tukipalvelut. Asiantuntijaverkosto on ryhmä paikallisia toimijoita, jotka tekevät Naturpolis Oy:n kanssa yhteistyötä yrityspalveluiden toteuttamiseksi. Lisäksi Naturpolis pitää yllä julkisesti saatavilla olevaa yritysrekisteriä, jossa listataan Kuusamossa, Taivalkoskella ja Posiolla toimivat yritykset ja niiden tietoja. (Naturpolis Oy 2018.)

Opinnäytetyön aloittamishetkellä yhtiössä työskenteli 15 työntekijää ja käynnissä olevia hankkeita oli 15. (Berit Lahtela, henkilökohtainen tiedonanto 13.2.2018.) Hankkeiden kautta Naturpolis Oy on tehnyt yhteistyötä useiden kumppaneiden kanssa. Yhteistyökumppaneina erilaisissa hankkeissa ovat olleet muun muassa Elinkeino-, liikenne- ja ympäristökeskus, Oulun yliopisto, Kajaanin ammattikorkeakoulu, Ruka-Kuusamo Matkailu ry, Metsähallitus ja Pohjois-Pohjanmaan liitto. (Naturpolis Oy 2018.)

Lähtökohdat tietosuoja-asetuksen suhteen

EU:n uusi tietosuoja-asetus astui voimaan 24.5.2016, ja sen soveltaminen alkaa 25.5.2018. Siirtymäajan aikana organisaatioiden on valmistauduttava täyttämään asetuksessa määritellyt vaatimukset. Naturpolis Oy:ssä on aloitettu alustava valmistelu vaadittavien toimenpiteiden täyttämiseksi vuoden 2017 aikana. Näihin valmisteluihin lukeutuvat muun muassa tutkittavien asioiden määrittely, aiheeseen liittyvä koulutustilaisuus henkilökunnalle ja tämän opinnäytetyön tilaus Kajaanin ammattikorkeakoululta. Lisäksi valmisteluissa on mukana lakiasiaintoimisto.

Naturpolis Oy on rekisterinpitäjä ja henkilötietojen käsittelijä, eli sillä on hallussa tietty määrä henkilötietoja erilaisissa muodoissa ja yhtiö käsittelee näitä henkilötietoja toimin-

nassaan. Lisäksi yhtiöllä on useita hankkeita ja yhteistyökumppaneita, joihin voi liittyä henkilötietojen käsittelyä. Osa henkilötietojen käsittelystä on ulkoistettua.

Naturpolis Oy:llä on asiakkaistaan rekisteri, johon asiakkailta voidaan kerätä muun muassa nimi, osoite, yhteystiedot ja syntymäaika. Lisäksi yritystä perustettaessa voidaan kysyä tarpeellisia lisätietoja. Näitä tietoja kerätään tietyissä tapauksissa, kun asiakas toimii Naturpolis Oy:n kanssa. Naturpolis ylläpitää myös Koillismaan yritysrekisteriä, johon tallennetaan tietoja Kuusamon, Taivalkosken ja Posion alueilla toimivista yrityksistä. Yritysrekisteri toimii julkisesti verkossa, ja sieltä löytyy yrityksiin liittyviä tietoja, kuten nimi, tuotteet, kotikunta, yritysmuoto, postitoimipaikka ja puhelinnumero. Yhtenä rekisterinä yhtiö ylläpitää myös uutiskirjeen postituslistaa, johon liitytään antamalla nimi ja sähköpostiosoite. Edellä mainituista rekistereistä kerrotaan tarkemmin rekisteriselosteessa, joka löytyy tämän työn liitteenä (liite 3).

Naturpolis Oy ylläpitää myös henkilöstörekisteriä, johon kuuluu yhtiön henkilökunta. Yhtiön henkilöstöltä kerätään muun muassa työllistymisen, palkanmaksun ja lomien käsittelyyn tarpeellisia tietoja. Henkilöstörekisteri ei ole saatavilla julkisesti, vaan se on tarkoitettu henkilökunnalle.

Yhtiön tietojärjestelmäpalvelut tuottaa LapIT Oy. Näihin palveluihin kuuluvat muun muassa IT-laitteiden toimitus, IT-tuki, ohjelmistojen toimitus ja levyjaon ylläpito. Levyjaolla säilytetään sähköisiä asiakirjoja, joihin voi lukeutua myös henkilötietoja. Tietyt järjestelmät, kuten palkanlaskentaan, lomiin, työmatkoihin tai kilpailutuksiin liittyvät palvelut ovat Kuusamon kaupungin toimittamia.

5 Työn toteutus

Tässä luvussa kuvaillaan tietosuoja-asetukseen liittyviä suosituksia, ehdotuksia ja ohjeistuksia, joita Naturpolis Oy:lle on tuotettu valmistautumisjakson aikana. Työn kaikki alkuperäiset tavoitteet, kuten tietotilinpäätöksen laatiminen, eivät toteutuneet. Näistä asioista voidaan kuitenkin tehdä jatkoa varten esimerkiksi toteuttamiselle suositus, jos se koetaan tarpeelliseksi.

5.1 Tietosuojavastaavan tarpeen määrittely

Tietosuojavastaava on organisaatiossa henkilö, joka valvoo tietosuoja-asetuksen ja tietoturvan toteutumista organisaatiossa ja on yhteishenkilönä näihin liittyvissä asioissa. Tietosuojavastaavan asema on riippumaton ja tuo mukanaan edellä mainitut tehtävät ja velvoitteet, joita vastaavan täytyy lain mukaan noudattaa. Nimitetty tietosuojavastaava voi kuitenkin suorittaa muitakin tehtäviä, kunhan ne eivät ole ristiriidassa tietosuojavastaavan velvollisuuksien kanssa.

Tietosuoja-asetuksessa on määritelty, että organisaatioon on nimitettävä tietosuojavastaava, jos

- organisaatio on julkisen sektorin toimija, joka ei ole tuomioistuin
- organisaation henkilötietojen käsittelyyn liittyvät ydintehtävät muodostuvat laajamittaisesta, säännöllisestä ja järjestelmällisestä seurannasta
- organisaation ydintehtävät muodostuvat erityisiin tietoryhmiin, rikostuomioihin tai rikoksiin liittyvästä henkilötietojen käsittelystä.

Koska Naturpolis ei täytä yhtäkään näistä kriteereistä, ei tietosuojavastaavan nimitys ole pakollista. Tällöin vastaavan nimittäminen jää vapaaehtoiseksi ja on pohdittava, että olisiko tietosuojavastaavan nimittäminen hyödyksi Naturpolis Oy:lle.

Ehdotetaan, että Naturpolis Oy:lle ei nimitetä tietosuojavastaavaa. Tätä perustellaan sillä, että yhtiön tietosuojan toiminnan kannalta tietosuojavastaavan nimittäminen ei toisi merkittävästi hyötyjä. Sen sijaan aseman laissa määritellyt velvoitteet monimutkaistaisivat tarpeettomasti organisaation toimintaa ja toisivat ylimääräistä työkuormaa.

Suositeltavissa on sen sijaan, että organisaatiossa nimitetään tietosuojan toteuttamisen vastuuhenkilö. Tämä henkilö toteuttaisi samanlaisia tehtäviä kuin tietosuojavastaava, mutta ilman vastaavaa koskevia velvoitteita. Nimitetty vastuuhenkilö olisi yhteyshenkilönä tietosuojaan liittyvissä asioissa ja toimisi tarpeen mukaan esimerkiksi rekisteröityjen ja valvontaviranomaisen kanssa. Vastuuhenkilöllä tulisi olla riittävä tuntemus tietosuojaan ja tietosuoja-asetukseen liittyvistä asioista.

Alustavasti Naturpolis Oy suunnittelee ottavansa käyttöön tietosuojaan liittyvän ja infosähköpostin, joiden kautta asiakkaat voivat ottaa yhteyttä tietosuojaan liittyvissä asioissa. Sähköpostin päässä ei ole yksittäistä nimitettyä vastuuhenkilöä, vaan alustavasti vastuu jaetaan usean työntekijän kesken. Tästä päätetään tarkemmin myöhemmin.

5.2 Tietotilinpäätös ja riskien arviointi

Naturpolis Oy:lle suositellaan perusteellisen tietotilinpäätöksen tekemistä. Tällä hetkellä yhtiöllä on melko hyvä kuva sen henkilötietoihin liittyvästä toiminnasta, mutta tarkempi dokumentointi kaikista tietovarannoista, niiden luonteesta, menettelytavoista, suojauksista ja oikeuksien toteuttamisesta voisi edesauttaa tietosuojan kehittämistä jatkossa. Tietotilinpäätöksen laatiminen oli yksi tämän työn tavoitteista, mutta sitä ei ehditty toteuttaa. Tietotilinpäätöksen tekoa kuitenkin suositellaan lähitulevaisuudessa ja sen toteuttamisessa voidaan käyttää luvussa 2.1 mainittuja kuvailuja.

Tietotilinpäätöksen aikana suositellaan myös riskien perusteellista arviointia. Riskien arvioinnissa pohditaan henkilötietoihin kohdistuvia riskejä. Riskien suuruuteen voivat vaikuttaa muun muassa käsiteltävien henkilötietojen määrä ja arkaluonteisuus sekä niihin kohdistuvat suojaustoimet. Riskien arvioinnissa voidaan käyttää esimerkiksi JUHTA-yhteishankkeen tarjoamaa Riskiarviointi-työkalua.

5.3 Rekisteriselosteet ja selosteet käsittelytoimista

Tietosuoja-asetukseen valmistautumisen myötä Naturpolis Oy:n rekisteriselosteita on päivitetty vastaamaan asetuksen vaatimuksia. Rekisteriselosteita on kaksi: henkilöstörekisterin rekisteriseloste ja asiakas- ja yritysrekisterin sekä uutiskirjeen rekisteriseloste. Näiden laatimisen toteutti asianajotoimisto.

Molemmissa rekisteriselosteissa kuvataan henkilötietojen käsittelyyn liittyviä asioita. Selosteet jakautuvat seuraaviin osioihin:

- Mitä tietoja kerätään.
- Miten ja millä perusteella kerättyjä tietoja käytetään.
- Miten kerättyjä tietoja jaetaan.
- Mitkä ovat rekisteröidyn oikeudet.
- Miten tietoturva toteutuu.
- Miten kauan tietoja säilytetään.
- Missä seloste on nähtävillä.

Asiakas- ja yritysrekisterin sekä uutiskirjeen rekisteriselosteessa on lisäkohtana kuvaus alaikäisten tietosuojasta.

Asiakas- ja yritysrekisterin sekä uutiskirjeen rekisteriseloste löytyy Naturpolis Oy:n verkkosivuilta ja myös tämän opinnäytetyön liitteenä (liite 3) Henkilöstörekisterin rekisteriseloste on tarkoitettu vain Naturpolis Oy:n henkilökunnan nähtäville ja se ei ole julkisesti saatavilla.

5.4 Tietoturvallisuus

Naturpolis Oy:n toimitiloissa on huolehdittu fyysisen tietoturvan perusasioista. Toimitiloissa pidetään ovet lukossa ja henkilökuntaa on neuvottu huolehtimaan salasanoistaan ja laitteistaan. Toimitiloissa valvotaan, että ulkopuoliset henkilöt eivät pääse vaeltelemaan esimerkiksi työhuoneisiin ilman syytä ja valvontaa. Tietoturvallisuus on kuitenkin asia, jota kannattaa kerrata aika ajoin. Lisäksi tietoturvaan liittyviä asioita kerrataan myöhemmässä koulutustilaisuudessa.

Naturpolis Oy:n tietojärjestelmäpalvelut toimittaa LapIT Oy. Tämän myötä myös tekninen tietoturva on LapIT Oy:n vastuulla. Tekniseen tietoturvaan kuuluvat muun muassa ohjelmistopäivityksistä huolehtiminen, verkkoliikenteen turvaaminen, varmuuskopiointi ja lokitukset. LapIT Oy:n palvelimilla säilytetään myös Naturpolis Oy:n tietoja ja se toimii täten myös henkilötietojen käsittelijänä. Onkin suositeltavaa, että LapIT Oy:ltä pyyde-

tään selvitystä siitä, että myös sen palvelut noudattavat EU:n tietosuoja-asetuksen vaatimuksia. Selvitykseen voidaan muun muassa pyytää tietoturvan toteuttamistapojen selittämistä. Myös Naturpolis Oy:n ja LapIT Oy:n välinen palvelusopimus tulisi käydä läpi ja varmistaa, että siinä sovitaan EU:n tietosuoja-asetuksen noudattamisesta.

5.5 Tietoturvaloukkauksista ilmoittaminen

Tietoturvaloukkauksien ilmoittamista varten on luotu yleiset ohjeet ja lomakkeet. Tavoitteena on ollut tehdä ilmoituksen tekemisestä mahdollisimman selkeää ja suoraviivaista niin, että tietosuoja-asetuksessa määriteltyä vaatimusta voidaan noudattaa. Tietoturvaloukkausten ilmoittamislomakkeen (liite 1) pohjana on käytetty Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) laatimaa pohjaa. Sitä on kuitenkin muokattu huomattavasti Naturpolis Oy:n tarpeisiin sopivammaksi.

Kun tietoturvaloukkauksen havaitaan tapahtuneen, ilmoitetaan tästä välittömästi esimiehelle. Tämän jälkeen esimiehen johdolla tietoturvaloukkaus analysoidaan huolellisesti ja samalla täytetään tietoturvaloukkausten ilmoittamiseen tarkoitettu lomake (liite 1). Tämän tulisi tapahtua ilman aiheetonta viivytystä. Kun tietoturvaloukkaukseen liittyvät seikat on käyty läpi ja lomake täytetty, toimitetaan lomake ilman aiheetonta viivytystä valvontaviranomaiselle.

Tietoturvaloukkauksista ja niiden ilmoittamisesta opastetaan tarkemmin nykyisille työntekijöille koulutuksessa. Uusille työntekijöille opastetaan tietoturvaloukkauksista ja niiden ilmoittamisesta tietosuojaperehdytyksen aikana. Lisäksi tietoturvaloukkauksista kerrotaan henkilötietojen käsittelyn ohjeistuksessa (liite 2). Ohjeistus laitetaan kaikkien työntekijöiden saataville levyjaolle. Pääasiallisena toimenpiteenä työntekijöitä opastetaan ottamaan välittömästi yhteyttä esimieheen.

5.6 Sopimukset ja alihankintaa ohjaavat periaatteet

Jos henkilötietoja käsitellään tai säilytetään sähköisessä muodossa ulkoisen palveluntuottajan toimesta, tulisi tietosuoja-asetukseen liittyvistä seikoista sopia toimeksiantosopimuksessa. Nykyisten sopimusten soveltuvuus kannattaakin varmistaa ja tarpeen mukaan muokata niitä vastaamaan tietosuoja-asetuksen vaatimuksia. Luvussa 3.8 käydään läpi asioita, joista sopimuksessa tulisi sopia. Naturpolis Oy:n kannalta ainakin LapIT

Oy:n kanssa tulisi selvittää, miten LapIT Oy noudattaa tietosuoja-asetusta, koska LapIT Oy:llä on Naturpolis Oy:n sähköisten tietojen ja teknisen tietoturvan kannalta merkittävä asema.

Myös tarjouspyynnöissä tietosuoja-asetus tulisi ottaa huomioon. Mahdollisten palvelun-tarjoajien on pystyttävä osoittamaan, että he noudattavat tietosuoja-asetusta. Tarjous-pyyntöä laadittaessa suositellaan huomioitavan ainakin luvussa 3.8 mainittuja seikkoja.

5.7 Rekisteröityjen oikeudet

Rekisteröidyillä on oikeus muun muassa saada tietoa Naturpolis Oy:n henkilötietojen käsittelystä. Yhtiön verkkosivuille tuodaan julkisesti näkyviin rekisteriseloste, jossa kerro-taan henkilötietojen käsittelystä. Rekisteröidyille asiakkaille tiedotetaan tästä rekisteri-selosteesta sähköpostitse ja henkilötietojen keruun yhteydessä. Lisäksi rekisteröidyillä on muita oikeuksia, joiden toteuttamiseksi kehiteltyjä ratkaisuja esitellään tässä luvussa.

5.7.1 Suostumus

Asiakkaiden henkilötietoja kerätään asianajotoimiston laatimalla asiakaslomakkeella, jossa pyydetään tietojen lisäksi suostumusta tietojen käsittelemiseen ja luovuttamiseen. Lomakkeessa ei ole valmiiksi ruksattuja kohtia ja asiakkaalta vaaditaan selvä suostu-mus. Lisäksi lomakkeessa kerrotaan, mistä rekisteriselosteen löytää verkossa sekä Na-turpolis Oy:n henkilötietojen käsittelyyn liittyville kysymyksille tarkoitetun sähköpostin osoite.

Suostumuksen pyytämisessä on tulevaisuudessa huomioitava myös asiakkaan ikä. Tie-tosuoja-asetuksen mukaan alle 16-vuotiaat henkilöt tarvitsevat vanhempien suostumuk-sen tietojen luovuttamiselle. Asetus antaa EU:n jäsenmaille mahdollisuuden laskea tätä ikärajaa 13 ikävuoteen asti lainsäädännössään, mutta tällä hetkellä 16 vuoden ikäraja näyttäisi olevan voimassa. Vanhempien suostumus pitäisi myös pystyä varmistamaan, joten suostumusta varten vanhempien pitäisi olla tietojen luovutushetkellä mahdollisesti läsnä tai vaihtoehtoisesti vanhempien suostumusta varten voisi luoda oman lomakepoh-jan.

5.7.2 Henkilötietoihin liittyvät pyynnöt

Naturpolis Oy:n on pyydettäessä toimitettava selvitys rekisteröidylle hänen tiedoistaan. Selvitys on toimitettava useimmiten kuukauden kuluessa. Vaikkei yhtiöllä olisikaan selvityspyynnön tekijästä kerättyjä henkilötietoja, on selvitys toimitettava kuukauden kuluessa. Selvityksessä mainitaan tällöin, että yhtiöllä ei ole pyynnön tekijän tietoja.

Tällä hetkellä suunnitelmana on, että selvityspyynnön tullessa henkilötietoselvitys tehdään manuaalisesti. Selvitys tulee tehdä ilman aiheetonta viivytystä, kuitenkin yhden kuukauden aikana. Henkilötietojen olemassaolo tarkastetaan asiakas- ja yritysrekisteristä sekä katsotaan, että onko pyynnön tekijä uutiskirjeen saaja. Jos pyynnön tekijä kuuluu henkilökuntaan, tarkastetaan tällöin tiedot henkilöstörekisteristä.

Jos pyynnön tekijän henkilöllisyyttä on syytä epäillä tai tämän henkilöllisyydestä ei muuten olla varmoja, voidaan häneltä pyytää lisätietoja henkilöllisyyden varmistamiseksi. On tärkeää, että selvitystä ei luovuteta henkilölle, jolla ei ole oikeutta siinä oleviin tietoihin. Tällöin mahdollisuutena on tietoturvaloukkaus.

Opinnäytetyön aikana on myös pohdittu lisätyökalujen hankkimista selvityspyyntöjä varten. Yhtenä ratkaisuna on esitetty Konica Minoltan dokoni FIND-ohjelmistoa, jonka avulla yhtiön levyjaolta pystyttäisiin etsimään tiettyihin henkilöihin liittyvät tiedot nopeammin ja yksinkertaisemmin. Tämä vaatisi jonkin verran lisäinvestointeja ja käyttöönottoa harkitaan myöhempänä ajankohtana tarkemmin.

5.7.3 Muut henkilötietoihin liittyvät pyynnöt

Rekisteröidyllä on myös muita oikeuksia, joista kerrotaan tarkemmin luvussa 3.7. Jos Naturpolis Oy:lle tulee pyyntöjä, joissa pyynnön tekijä haluaa käyttää näitä oikeuksia, tulee pyynnöt ottaa käsittelyyn ilman aiheetonta viivytystä. Jos pyyntöjen toteuttamiselle ei ole pätevää estettä, toteutetaan ne normaalisti ja pyynnön tekijälle ilmoitetaan tästä.

5.8 Henkilötietojen käsittelyn ohjeistus

Naturpolis Oy:n henkilökuntaa on tiedotettu tietosuoja-asetuksesta hyvissä ajoin. Aiheesta on järjestetty myös henkilökunnalle koulutuksia aikaisemmin. Tämän opinnäyte-

työn tuloksena on luotu muistilista ja ohjeistus henkilötietojen käsittelijöille (liite 2). Lisäksi tämän opinnäytetyön tuloksia esitellään myöhemmässä koulutustilaisuudessa nykyiselle henkilökunnalle.

Uusille ja vanhoille työntekijöille suositellaan arjentietosuoja.fi-sivuston materiaaliin tutustumista. Kyseinen sivusto on JUHTA-yhteishankkeen tietosuoja-asetusta varten tuottama ja sieltä löytyy aiheeseen liittyen muun muassa opastavaa videomateriaalia, joka soveltuu kaikille henkilötietojen käsittelijöille..

5.9 Tulevaisuus

Sisäänrakennetun tietosuojan periaate tarkoittaa sitä, että tietosuoja huomioidaan henkilötietojen käsittelyn jokaisessa vaiheessa. Tämä merkitsee sitä, että tietosuoja-asetuksen periaatteet pitää huomioida myös tulevaisuudessa kaikessa henkilötietojen käsittelyyn liittyvässä toiminnassa, kuten esimerkiksi tarjouspyynnöissä, hankinnoissa, henkilötietojen käsittelyä vaativissa hankkeissa tai uusien työntekijöiden palkkaamisessa ja kouluttamisessa. Tietosuoja on myös asia, jota voi lähes aina kehittää paremmaksi erilaisilla keinoilla.

Naturpolis Oy on alustavasti suunnitellut, että tietosuojan toteutumista valvotaan tekemällä tietyin väliajoin tietosuojaan liittyviä katsauksia. Katsausten avulla tietosuojan toteutumisen valvomisen lisäksi voitaisiin löytää mahdollisia keinoja tietosuojan parantamiseksi. Tällaisiin projekteihin voitaisiin palkata ulkoinen tietosuoja-asiantuntija tekijäksi.

Tietosuojakatsaukset olisivat hyödyllisiä myös mahdollisen muuttuvien linjausten takia. Tietosuoja-asetus jättää tietyissä asioissa EU:n jäsenmaille lainsäädännössä kansallista liikkumavaraa ja tulevaisuudessa luultavasti tehdään tietosuoja-asetukseen liittyviä tulkintalinjauksia, jotka mahdollisesti voivat muokata yleisiä käytänteitä. Tilannetta suositellaan seuraamaan myös mahdollisten tietosuojakatsausten ulkopuolellakin. Hyvänä tiedonlähteenä tietosuojaan liittyvissä uutisissa toimii vastaavaisuudessakin Suomen tietosuojavaltuutetun toimisto.

6 Pohdinta

Opinnäytetyön alkuvaiheessa minulla ei ollut kovinkaan tarkkaa tietoa EU:n yleisen tietosuoja-asetuksen sisällöstä. Opintojeni kautta olin tutustunut tietoturvan periaatteisiin, mutta varsinaiseen lainsäädäntöön en ollut koskaan perehtynyt tarkemmin. Työn alussa kävimme Naturpolis Oy:n edustajan kanssa alustavasti läpi tietosuoja-asetuksen sisältöä ja sen merkitystä yhtiölle. Työn alkupuolilla kävin Kuusamossa yhtiön toimitiloissa, jossa pääsin tutustumaan muutaman päivän ajan yhtiön toimintaan ja työntekijöihin. Lisäksi vierailun aikana osallistuin tietosuoja-asetukseen liittyvään koulutustilaisuuteen, jonka järjesti Asianajotoimisto Kontturi & Co Oy.

Vierailun jälkeen työ jatkui aiheeseen liittyvään kirjallisuuteen perehtymällä ja teoriaosuuden kirjoittamisella. Osallistuin myös Kasvua Kainuuseen -hankekokonaisuuden järjestämään tietosuojakoulutukseen, josta sain työtäni varten lisätietoa ja materiaalia. Tietosuoja-asetuksen opettelu onnistui asetuksen sisältöä lukemalla ja samalla peilaamalla sitä muiden asiantuntijoiden tulkintoihin sen sisällöstä.

Teoriaosuuden kirjoittamisen jälkeen siirryin pohtimaan opitun soveltamista Naturpolis Oy:n toimintaa varten. Jaoin alustavasti tietosuoja-asetuksen vaatimukset kymmeneen eri kohtaan, joita lähdin yksitellen ratkomaan. Tuloksina syntyi selvityksiä ja ohjeistuksia, kerrotaan tarkemmin luvussa 5. Osa toteutuneista ohjeistuksista löytyy tämän työn liitteinä.

Työn aikana pidin yhteyttä Naturpolis Oy:n edustajaan noin 2–3 viikon välein. Keskusteluissamme tarkasteltiin työn etenemistä ja sovimme seuraavista työhön liittyvistä tehtävistä. Toimeksianto muuttui ja tarkentui työn edetessä jatkuvasti. Tietosuoja-asetukseen valmistautumisessa oli mukana lakiasiaintoimisto, jonka toimesta muun muassa päivitettiin rekisteriselosteet. Työn edetessä jotkin tietosuoja-asetuksen tavoitteista toteutettiin opinnäytetyön ulkopuolella, jolloin pääsin työssä keskittymään tarkemmin muihin vaatimuksiin.

Opinnäytetyön kaikki tavoitteet eivät täysin toteutuneet. Alussa oli tarkoituksena tehdä tarkka tietotilinpäätös yhtiön henkilötietojen käsittelystä ja laatia rekisteriselosteet sekä selostus henkilötietojen käsittelystä. Tietotilinpäätöksen tekeminen etänä osoittautui ongelmalliseksi ja vaikka yhtiöllä on melko selkeä kuva henkilötietojen käsittelytoimistaan, olisi perusteellisen tietotilinpäätöksen tekeminen suositeltavaa. Opinnäytetyöhön kirjoi-

tettiin ohjeita tietotilinpäätöksen tekemiseen ja yhtiöllä on tietotilinpäätöstä varten pohja, jonka avulla sitä voi tulevaisuudessa alkaa laatimaan.

Vaikka työn toteuttamisessa olisi ollut parantamisen varaa, olen työhön silti tyytyväinen. Työn aikana pääsin tutustumaan syvällisesti hyvin ajankohtaiseen aiheeseen ja sain ohjeistaa ja avustaa toimeksiantajaa siihen liittyen. Tiukkaan aikatauluun nähden työ eteni hyvää tahtia. Lainsäädäntö aihepiirinä on minulle ollut haastavaa ja olikin yllättävää, miten hyvin teoriaosuuden toteuttaminen sujui. Parannettavia asioita työn toteuttamisessa omalta kannalta olisivat olleet parempi suunnittelu, suunnitelman tarkempi seuraaminen ja oma-aloitteisuuden parantaminen.

Opinnäytetyön tuloksena syntyi joukko ohjeistuksia ja suosituksia, joita voidaan hyödyntää tietosuoja-asetuksen noudattamisessa. Tulevaisuudessa yhtiön tietosuojan kehitystä kannattaa seurata. Samoin myös lainsäädännön kehitystä kannattaa seurata. Tietosuoja-asetukseen tehdään mahdollisesti tulevaisuudessa tulkintalinjauksia, jotka voivat vaikuttaa tietosuojakäytänteisiin.

Lähteet

A 2016/679. Tietosuoja-asetus. Saatavilla http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Ala-Varvi, J. Tietosuoja-asetuksen (GDPR) vaatimusten käyttöönotto. Saatavilla 6.5.2018 https://www.tietosuojakuntoon.fi/files/tietosuoja_yhteenveto.pdf

Hämäläinen, J. (2017). Tietosuoja-asetuksen sopimusvaatimukset ja vaikutus tarjous-pyynnön suunnitteluun. Saatavilla 6.5.2018 https://www.kuntaliitto.fi/sites/default/files/media/file/TietosuojaKilpailutuksessa_Hamalainen.pdf

JUHTA. (2.11.2017). *Johdon ja esimiesten tietosuojakoulutusvideo*. Saatavilla 6.5.2018 https://vimeo.com/234313084/f874f6b947

Karjalainen, H. (27.2.2018). Tietosuojakoulutus. [Luento]. Sotkamo: OP Kainuu

L 523 / 1999. Henkilötietolaki. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Laakso, M. (N.d). Tietoturvallisuuden peruskäsitteitä. Saatavilla 6.5.2018 https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvallisuuden-peruskasitteita

Mäkelä, P. (13.2.2018). Tietosuoja yritystoiminnassa. [Luento]. Kuusamo: Naturpolis Oy

Naturpolis Oy. (2018). Saatavilla 6.5.2018 http://www.naturpolis.fi/fi/

Rousku, K. (toim.) (2017). Ohje riskienhallintaan. Saatavilla http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

Talus, A., Autio, E., Hänninen, A., Pihamaa, H., Kantonen, S., tietosuojavaltuutetun toimisto. (2017). Miten valmistautua EU:n tietosuoja-asetukseen?. Saatavilla 6.5.2017 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimisto. (2010). Ota oppaaksi henkilötietolaki!. Saatavilla 6.5.2018

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq7xbJn/Ota_oppaaksi_henkilotietolaki_teksti.pdf

Tietosuojavaltuutetun toimisto. (2012). Laadi Tietotilinpäätös. Saatavilla 6.5.2018 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Tietosuojavaltuutetun toimisto. (2017a). Henkilötietojen tietoturvaloukkaukset. Saatavilla 6.5.2018 http://tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/johtavavalvontaviranomainen.html

Tietosuojavaltuutetun toimisto. (2017b). Johtavan valvontaviranomaisen määrittely. Saatavilla 6.5.2018 http://tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/johtavavalvontaviranomainen.html

Tietosuojavaltuutetun toimisto. (2018). Sanastoa tietosuojauudistukseen liittyen. Saatavilla 6.5.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html

Valtiovarainministeriö. (2016). EU-tietosuojan kokonaisuudistus. Saatavilla 6.5.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Valtiovarainministeriö. (2018). Yhteishankkeiden materiaalit. Saatavilla 6.5.2018 http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

Vanto, J. (2011). *Henkilötietolaki käytännössä.* Saatavilla https://kamk.finna.fi/, Alma Talent Verkkokirjahylly

Suomen tietosuojapalvelut Oy. (N.d). Periaatteet, politiikat ja suunnitelmat. Saatavilla 6.5.2018 https://opitietosuojaa.fi/index.php/fi/49-tyokalupakki/periaatteet-politiikat-ja-suunnitelmat

Suomen tietosuojapalvelut Oy. (N.d). Tietosuoja. Saatavilla 6.5.2018 https://opitietosuojaa.fi/fi/aloitus/tietosuoja

Suomen yrittäjät. (2018). Yrittäjän tietosuojaopas. Saatavilla 6.5.2018 https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018_130418.pdf

U.S. Department of Commerce. (2018a). Privacy Shield list. Saatavilla 6.5.2018 https://www.privacyshield.gov/list

U.S. Department of Commerce. (2018b). Program Overview. Saatavilla 6.5.2018 https://www.privacyshield.gov/Program-Overview

naturpolis
NORDIC BUSINESS CENTER

1 Yhteystiedot tietoturvaan liittyen

***Sähköposti**:* info@naturpolis.fi

Täydennä alla olevat tiedot, kun olet havainnut henkilötietojen tietoturvaloukkauksen.

Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

2 Perustiedot tietoturvaloukkauksesta

(a) Kuvaa tietoturvaloukkausta kaiken saatavissa olevan tiedon perusteella.

(b) Milloin tietoturvaloukkaus tapahtui?

(c) Miten tietoturvaloukkaus tapahtui?

(d) Mikäli tämä ilmoitus tehdään säädetyn määräajan ulkopuolella, ilmoita perustelut tälle.

(Mahdollisuuksien mukaan ilmoitus on tehtävä 72 tunnin kuluessa sen ilmitulosta valvontaviranomaiselle)

Ilmoittajan tiedot:_____

Sähköposti:_____Puhelin:_____

Lähetä ilmoitus: info@naturpolis.fi

naturpolis
NORDIC BUSINESS CENTER

Ohjeita henkilötietojen keräämistä ja käsittelyä varten

- Henkilötietojen keräämiseen tulee aina olla pätevä, lainmukainen ja läpinäkyvä syy.
- Kerättyjä tietoja saa vain ja ainoastaan käyttää niihin tarkoituksiin, mihin ne on alun perin kerätty. Jos tietoja halutaan käyttää millään muulla tavalla, tulee asiakkaalta saada tätä varten suostumus.
- Älä kerää tietoja turhaan äläkä kerää henkilötietoja, jotka ovat epäolennaisia toimintasi kannalta.
- Huolehdi, että kerätty tieto on täsmällistä
- Asiakkailla on oikeus tietää, mihin kerättäviä tietoja käytetään. Ole valmis perustelemaan henkilötietojen keräämisen syyt ja ohjaa asiakas Naturpolis Oy:n tietosuojaselosteeseen
- Henkilötietoja kerätessä on tärkeä saada asiakkaan suostumus. Suostumus voidaan osoittaa lomakkeissa esimerkiksi ruksattavalla kohdalla (ei saa olla valmiiksi ruksattu!)
- Tiedon elinkaari. Kuinka kauan henkilötietoja säilytetään? Kuinka kauan tarvitsee säilyttää? Henkilötietoja on säilytettävä ainoastaan niin kauan kuin on tarpeen.
- Ole huolellinen kerättyjen henkilötietojen kanssa. Huolehdi, että tiedot eivät joudu asiaankuulumattomien nähtäville. Tietoja on säilytettävä niin, että tietojen eheys ja luottamuksellisuus säilyy tiedon koko elinkaaren ajan.
- Jos havaitset tietoturvaloukkauksen, ilmoita tästä välittömästi esimiehelle.

Työntekijöiden suositellaan tutustuvan https://arjentietosuoja.fi sivuston materiaalin ja nettitestiin. Materiaali sisältää hieman alle kahden tunnin verran videota, jossa käydään läpi mm. tietosuoja-asetuksessa käsiteltäviä asioita ja tietosuojan periaatteita.

Nettitesti on kymmenen satunnaisen kysymyksen pituinen testi, jossa testataan tietämystä videoilla läpikäydyistä asioista. Testi on uusittavissa niin monta kertaa kuin haluaa ja koska kysymykset vaihtuvat testien välillä jonkin verran, on useampi testikerta suositeltavaa.

naturpolis
NORDIC BUSINESS CENTER

ASIAKAS- JA YRITYSREKISTERIN SEKÄ UUTISKIRJEEN REKISTERISELOSTE

Päivitetty 11.4.2018

Rekisterinpitäjä

Henkilötietolain (523/1999) tarkoittama henkilötietojen rekisterinpitäjä:

Koillis-Suomen kehittämisyhtiö Naturpolis Oy
Nuottatie 6 A, 93600 Kuusamo, y-tunnus 1940705-4

Rekisteriasioinnin yhteystiedot

info@naturpolis.fi

Rekisterien nimet

Asiakasrekisteri, yritysrekisteri sekä uutiskirjeen tilaajarekisteri.

Tässä selosteessa kuvataan ne periaatteet, joiden mukaan Naturpolis Oy kerää, käyttää, suojaa ja luovuttaa asiakkaiden henkilötietoja.

Tämä seloste ei sovellu yhteistyötahoihimme (hankerahoittajat, viranomaiset). Pyydämme katsomaan yhteistyötahojemme selosteet siitä, miten he käyttävät asiakastietoja.

1. Keräämämme tiedot

Voimme kerätä henkilötietojasi, mikäli vierailet yrityksessämme, käytät palvelujamme, osallistut järjestämiimme tilaisuuksiin tai tapahtumiin, tilaat uutiskirjeen tai muutoin olet yhteydessä meihin.

Voimme yhdistää suoraan meille antamiasi tietoja keräämiimme tietoihin sekä muista lähteistä keräämiimme tietoihin.

Keräämiämme henkilötietoja ovat nimi, posti- ja sähköpostiosoite, puhelinnumero, syntymäaika, kotisivut tai Facebook-sivut, yrityksen perustamistilanteessa henkilötunnus; asiointi- ja käyttötiedot, kuten tiedot ilmaisista tai maksullisista palveluista. Tiedot, joita olet tallentanut verkkopalveluun.

Voimme kerätä tietojasi julkisista viranomaisrekistereistä (esimerkiksi patentti ja – rekisterihallituksen yritystietojärjestelmä (YTJ)) ja muuten julkisesti saatavilla olevaa tietoa.

Voimme esimerkiksi kerätä tietoa sinusta, jos olet yhteydessä meihin sosiaalisen median välityksellä.

2. Miten ja millä perusteella käytämme keräämiämme tietoja

Voimme käyttää tietoja suorittaaksemme palveluja sinulle sekä käsitelläksemme palveluitamme koskevat maksut, kertoaksemme sinulle palveluistamme, hankkeistamme tai erityistapahtumista, jotka voivat kiinnostaa sinua (jos et kiellä suoramarkkinointia).

Voimme käyttää tietoja kertoaksemme sinulle yhteistyökumppaneidemme tuotteista ja palveluista (jos et kiellä suoramarkkinointia); yhteydenpitoon liittyen pyyntöihin, palveluihin, kysymyksiin ja kommentteihin.

Käytämme tietoja liiketoimintamme hoitamiseksi, mukaan lukien uusien palveluiden kehittäminen, asiakastutkimusten toteuttaminen, sekä myynti, markkinointi ja mainonta ja niiden tehokkuuden arvioiminen.

Käytämme tietoja palveluidemme, verkkopalveluidemme ja muun teknologiamme ylläpitämiseksi, hallitsemiseksi ja kehittämiseksi.

Käytämme tietoja petoksilta ja muilta rikoksilta, vaatimuksilta ja vastuilta suojautumiseksi ja niiden tunnistamiseksi ja ennaltaehkäisemiseksi sekä sovellettavan lain noudattamiseksi.

Voimme käyttää henkilötietojasi muillakin tavoilla, joista kerromme sinulle tietoja kerättäessä tai silloin, kun pyydämme suostumustasi tietojen käsittelyyn.

Henkilötietojen käsittelyperusteena on suostumus, sopimus ja oikeutettu etumme, joka perustuu osapuolten väliseen asialliseen yhteyteen (asiakassuhteen hoitaminen).

3. Miten jaamme keräämiämme tietoja

Yritys ei myy henkilötietojasi. Yritys luovuttaa tietojasi vain siten, kuin tässä selosteessa on kuvattu.

Henkilötietojasi voidaan luovuttaa yhteistyökumppaneille palvelun suorittamiseksi tai rahoituksen saamiseksi (esimerkiksi elinkeinoyhtiön hankkeiden rahoittajaviranomaiset, Ely-keskus).

Meillä on oikeus käyttää tai luovuttaa tietoja, mikäli se on tarpeen lain, säädöksen tai laillisen pyynnön johdosta, teknologian suojaamiseksi, oikeusvaateilta puolustautumiseksi tai niiden esittämiseksi, organisaatiomme, työntekijöidemme tai yleisön oikeuksien, etujen tai turvallisuuden suojaamiseksi tai petoksen, muun rikoksen tai sääntöjemme rikkomisen tutkimisen yhteydessä.

Emme siirrä tai luovuta missään tilanteessa tietoja EU-alueen ulkopuolelle.

4. Alaikäisten tietosuoja

Yritys käsittelee huoltajan suostumuksella alaikäisten yritysten perustajien ja arvontaan osallistuvien alaikäisten seuraavia henkilötietoja: nimi, yhteystiedot, koulutus, syntymäaika, osoitetiedot.

5. Oikeutesi

Sinulla on oikeus tarkastaa, mitä sinua koskevia tietoja rekisteriin on tallennettu. Tarkastuspyyntö tulee lähettää sähköpostitse: info@naturpolis.fi. Tarkastuspyyntö voidaan tehdä myös henkilökohtaisesti rekisterinpitäjän luona.

Sinä hallitset kaikkia henkilötietoja, jotka annat meille. Jos missään vaiheessa haluat korjata henkilötietojasi, ota meihin yhteyttä. Lisäksi sinulla on tietyissä tilanteissa oikeus pyytää sinua koskevien henkilötietojen poistamista rekisteristä sekä pyytää niiden siirtämistä toiselle yritykselle. Sinulla on oikeus rajoittaa henkilötietojen käsittelyä ja vastustaa henkilötietojen käsittelyä.

Pyydämme kuitenkin huomioimaan, että tietojen antaminen ja käsittelyn salliminen voi tietyissä tilanteissa olla palvelun käyttöönoton tai käyttämisen edellytys. Yritys varaa oikeuden keskeyttää palveluiden tarjoaminen tai estää pääsyn palveluihin, mikäli rekisteröity ei anna palvelun kannalta olennaisia tietoja tai vaatii niiden poistamista.

6. Tietoturva

Olemme sitoutuneet huolehtimaan asianmukaisista toimenpiteistä pitääksemme henkilötietosi turvassa. Tekniset, hallinnolliset ja fyysiset prosessimme on suunniteltu suojaamaan henkilötiedot vahingossa tapahtuvalta, laittomalta tai luvattomalta häviämiseltä, tietoihin pääsyltä, luovuttamiselta, käytöltä, muuttamiselta tai tuhoamiselta. Vaikka huolehdimme järjestelmiemme suojaamisesta, emme kuitenkaan voi taata, että internet-sivu, tietokonejärjestelmä tai tietojen siirto internetin tai muun julkisen verkon välityksellä on täysin turvallinen.

7. Yritysrekisterin tietojen tarkistaminen ja muiden henkilötietojen tarkistaminen

Tarkistamme vuosittain yritysrekisterin ajantasaisuuden YTJ:n tietojen perusteella.

Kun olemme yhteydessä sinuun, tarkistamme sinulta, ovatko tietosi muuttuneet.

8. Henkilötietojen säilyttäminen

Säilytämme henkilötiedot vain niin kauan kuin tietoja voidaan pitää tarpeellisina tässä selosteessa kuvattujen käyttötarkoitusten kannalta, ellei tietojen säilyttäminen tätä pidempään ole lain edellyttämä, hankerahoittajan edellyttämä tai lain nojalla sallittu.

Hankkeeseen liittyvät tiedot säilytetään hankepäätöksissä määritetyn ajankohtaan saakka.

Mikäli yrityksesi on poistettu yritysrekisteristä, poistamme yritystiedot ja henkilötiedot yritysrekisteristä kerran vuodessa.