KARELIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutusohjelma

Iiro Hirvonen

GDPR PIENYRITTÄJÄN NÄKÖKULMASTA

Opinnäytetyö
Lokakuu 2018

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Lokakuu 2018** **Tieto- ja viestintätekniikan koulutusohjelma** Tikkarinne 9 80200 JOENSUU (013) 260 600

Tekijä(t)
Iiro Hirvonen

Nimeke
GDPR pienyrittäjän näkökulmasta

Toimeksiantaja
Karelia-ammattikorkeakoulu, KoDa-hanke

Opinnäytetyön tavoitteena oli tutustua EU:n uuteen tietosuoja-asetukseen sekä selvittää, millaisia velvoitteita se tuo pienyrittäjille. Tutkimus tehtiin Karelia-ammattikorkeakoulun toimeksiannosta.

Työ toteutettiin tutkimalla tietosuoja-asetusta ja selventämällä sen sisältöä. Pienyrittäjän velvoitteita tarkasteltiin myös esimerkki yrityksessä.

Tietosuoja-asetusta tutkittaessa tuli ilmi, että asetus koskee kaikkia yrityksiä, pieniä poikkeuksia lukuun ottamatta. Jos yritys kerää asiakkaistaan henkilötietoja, joista asiakas voidaan tunnistaa, ja pitää niistä rekisteriä, koskevat tietosuoja-asetuksen tuomat velvoitteet yritystä.

Kieli	Sivuja 24
suomi	Liitteet 1
	Liitesivumäärä 6

Asiasanat

GDPR, tietosuoja, pienyritys

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
October 2018
Degree Programme in
Information Technology

Tikkarinne 9
80200 JOENSUU
FINLAND
+358 13 2260 600

Author (s)
Iiro Hirvonen

Title
General Data Protection Regulation (GDPR) from the Viewpoint of Small-sized Business.

Commissioned by
KODA project by Karelia University of Applied Sciences

This goal of this thesis was to get acquainted with the EU's new Data Protection Regulation and to find out what kind of obligations it brings to small enterprises. The study was carried out in Karelia University of Applied Sciences.

The thesis was carried out by examining the Data Protection Regulation and finding out its content. The small entrepreneur's obligations are also studied in the example enterprise.

Data Protection Regulation affect all businesses, with small exceptions. If a company collects personal information of its customers, which the customer could be identified, and keeps a register of this information's, affect the Data Protection Regulation enterprise.

Language
Finnish

Pages 24
Appendices 1
Pages of Appendices 6

Keywords
GDPR, data protection, small- and medium size enterprise

Sisältö

Liitteet

Liite 1. EU:n tietosuoja-asetus. PowerPoint-esitys

Lyhenteet ja termit

GDPR	General Data Protection Regulation eli Euroopan unionin vuonna 2016 voimaan tullut tietosuojalaki.
Henkilötieto	Tieto, josta tietty henkilö voidaan tunnistaa (yksilöidä), nimi, osoite, henkilötunnus, puhelinnumerot, luottokortin numerot.
Henkilötietojen käsittelijä	Palveluntarjoaja, joka käsittelee henkilötietoja.
Luonnollinen henkilö	Henkilö, joka on elossa ja olemassa.
Pienyritys (Pk-yritys)	Yritys, jossa alle 50 työntekijää.
Rekisterinpitäjä	Henkilötietorekisterin ylläpitäjä.
Rekisteröity	Henkilö, jonka henkilötietoja on yrityksen tai organisaation järjestelmissä.
SIEM	Security Information and Event Management, järjestelmä, jolla kerätään tietoa tietojärjestelmien tapahtumista.

1 Johdanto

Tässä opinnäytetyössä käsitellään, mikä on GDPR (General Data Protection Regulation) eli EU:n tietosuoja-asetus, mitä velvoitteita se tuo henkilötietojen käsittelyyn ja millaisia sanktioita asetuksen noudattamatta jättämisestä seuraa sekä käydään läpi, millaisia velvoitteita asetuksen voimaantulo tuo pienyrittäjille.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista. Henkilön tietoja, joista kyseinen henkilö voidaan tunnistaa, on suojattava väärinkäytöltä sekä kyseiset tiedot on pidettävä salassa. Tietosuoja ei siis ole sama asia kuin tietoturva. Tietoturvalla tarkoitetaan fyysisten laitteiden ja sovelluksien suojaamista kyberuhkilta, kuten viruksilta ja tietomurroilta. Suomessa tietosuoja on osa perustuslakia.

Opinnäytetyön toimeksiantajana oli Karelia-ammattikorkeakoulu. Karelia-AMK toimii hallinnoijana KoDa (Kokonaisvaltainen datan hallinnointi ja hyödyntäminen) -hankkeessa, johon opinnäytetyö liittyy.

Opinnäytetyön tavoitteena oli tutustua EU:n tietosuoja-asetukseen ja selvittää, miten se vaikuttaa pienyrittäjään ja millaisia velvoitteita asetus tuo pienyrittäjälle. Opinnäytetyön pohjalta tehdään tiivistetty visuaalinen esitelmä tietosuoja-asetuksen velvoitteista. Esitys löytyy liitteenä tämän opinnäytetyön lopusta.

2 GDPR

Euroopan unioni hyväksyi toukokuussa 2016 uuden tietosuoja-asetuksen. Asetusta on alettu soveltaa 25. toukokuuta 2018 alkaen. Henkilötietojen käsittelyn tulee jo noudattaa tätä uutta tietosuoja-asetusta [1.]

Tietosuoja-asetus uudistaa sääntelyä, joka koskee tietosuojaa. Asetuksella lisättiin henkilötietojen avoimuutta sekä parannettiin rekisteröityjen (henkilö, jolla on henkilötietoja yrityksen/organisaation järjestelmissä) oikeuksia, joilla he voivat valvoa henkilötietojensa käsittelyä [1.] Suomessa tietosuoja-asetuksen noudattamista valvoo tietosuojavaltuutettu ja tietosuojalautakunta [10].

Suomen nykyiseen tietosuojalakiin (perustuu EU-direktiiviin 95/46/EY) verrattuna uusi tietosuojalaki tuo muutamia parannuksia rekisteröityjen oikeuksiin. Rekisteröityjen oikeus tietää, mitä tietoja heistä on yrityksellä ja oikeus virheellisten tietojen korjaamiseen parantui. Lisäksi rekisteröidyn pyyntöön tietojensa poistamisesta tulee lisää säännöksiä sekä rekisteröidylle tulee oikeus siirtää tietonsa tietojärjestelmästä toiseen. Yrityksille uuden asetuksen suurin uudistus on tietosuojavastaavan nimeäminen, sekä ilmoitusvelvollisuus tapahtuneesta tietosuojaloukkauksesta [8.]

2.1 Henkilötietojen käsittely ja keräys

Luonnollisten henkilöiden henkilötietojen käsittelyn tulee olla lain mukaista ja perustua rekisteröidyn suostumukseen. Henkilötietojen keräämisen menetelmät ja kerättyjen henkilötietojen käytön pitäisi olla läpinäkyvää luonnolliselle henkilölle. Läpinäkyvyyden varmistamiseksi henkilön henkilötietojen käsittelyä koskevat tiedot olisi oltava helposti saatavilla ja niiden tulee olla kirjoitettu selkokielellä. Henkilötietojen riskeistä, säännöistä, suojatoimista ja oikeuksista tulisi ilmoittaa luonnolliselle henkilölle. Heillä on myös oikeus saada vahvistus ja ilmoitus heidän henkilötietojensa käsittelystä [2, kohta 39.]

Henkilötietoja kerättäessä tulee määritellä, mihin käyttötarkoitukseen tietoja kerätään ja minkälainen tietojenkäsittely on väittämätöntä [2, kohta 39]. Rekisterinpitäjä toimittaa rekisteröidylle lisätiedot, joita vaaditaan asianmukaiseen ja avoimeen käsittelyyn. Rekisteröidylle ilmoitetaan myös, onko hänen pakko toimittaa henkilötietoja ja mitä seuraa, jos tietoja ei toimiteta [2, kohta 60.] Henkilötietojen säilyttämiselle tulisi määritellä

säilytysaika, jonka tulisi olla mahdollisimman lyhyt. Säilytysajalla varmistetaan, että henkilötietoja ei säilytetä pidempään kuin on tarpeen. [2, kohta 39] Henkilötietojen lyhyellä säilytysajalla on tarkoitus poistaa turhia rekistereitä, joissa voi olla vanhentuneita henkilötietoja [9].

Henkilötietojen käsittely perustuu suostumukseen, jonka rekisteröitynyt henkilö on antanut vapaaehtoisesti. Henkilötietorekisterinpitäjän tulisi pystyä osoittamaan rekisteröidyn suostumus. Rekisteröidyn tulee olla tietoinen, millainen suostumus on kyseessä, ennalta muotoiltu ilmoitus suostumuksesta tulee olla helposti ymmärrettävässä ja saatavilla olevassa muodossa. Ilmoituksen pitää olla myös selkeällä ja yksinkertaisella kielellä kirjoitettu eikä ilmoitukseen saa sisällyttää kohtuuttomia ehtoja [2, kohta 42.]

Tietoisen suostumuksen antamiseksi rekisteröidyn on tiedettävä rekisterinpitäjästä henkilöllisyys ja se, mitä varten rekisteröidyn tietoja on käsitellä. Rekisteröidyn antama suostumus ei ole vapaaehtoinen, jos rekisteröidyllä ei ole mahdollisuutta vapaaseen valintaan tai rekisteröity ei voi kieltäytyä suostumuksen antamisesta [2, kohta 42.] Esimerkiksi jos henkilö rekisteröityy johonkin verkkopalveluun, palvelun ehtoja ei saisi olla valmiiksi hyväksyttynä, vaan henkilön pitää itse hyväksyä kyseisen palvelun ehdot.

Tietosuoja-asetus koskee kaikkia yrityksiä ja organisaatioita, jotka käsittelevät toiminnassaan henkilötietoja sekä niitä, jotka käsittelevät henkilötietoja tai pitävät henkilötietorekisteriä. Asetusta tulee soveltaa myös sellaisissa tapauksissa, joissa rekisterinpitäjä tai henkilötietojen käsittelijä on Euroopan unionin ulkopuolella ja käsittelee Euroopan unionin kansalaisen henkilötietoja [2, kohta 24.]

Henkilötietojen käsittely muihin kuin alkuperäiseen tarkoitukseen tulisi sallia vain, jos se sopii yhteen alkuperäisen käyttötarkoituksen kanssa. Rekisteröidyn henkilötietojen käyttö myöhempiin tarkoituksiin, esim. tilastotutkintaan, on mahdollista rekisteröidyn suostumuksella tai kyseisen rekisteröidyn tietojenkäsittely perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön. Rekisteröidylle tulee ilmoittaa hänen henkilötietojensa myöhemmästä käytöstä sekä hänen oikeuksistaan, kuten rekisteröidyn oikeudesta vastustaa henkilötietojensa käsittelyä [2, kohta 50.] Tietosuoja-asetus ei kuitenkaan kumoa muita henkilötietojen keräämiseen tarkoitettuja lakeja, esimerkiksi yrityksellä on oikeus säilyttää tietyn henkilön henkilötietoja kirjanpidon vuoksi, mutta kyseisten tietojen näkyvyyttä on rajoitettava [8.]

Rekisterinpitäjän oikeus on ilmoittaa rekisteröidyn mahdollisista rikollisista teoista tai yleiseen turvallisuuteen liittyvistä asioista ja luovuttaa kyseessä olevan rekisteröidyn henkilötiedot viranomaisille. Tietojen luovuttaminen on kuitenkin kiellettyä, jos ”tietojenkäsittely on ristiriidassa johonkin oikeudelliseen, ammatilliseen tai muuhun sitovaan salassapitovelvollisuuteen nähden.” [2, kohta 50.]

Rekisterinpitäjää ei saisi velvoittaa hankkimaan lisätietoja luonnollisesta henkilöstä, jos rekisterinpitäjä ei pysty tunnistamaan kyseistä luonnollista henkilöä hänellä olevien henkilötietojen perusteella. Rekisteröidyn antamista lisätiedoista rekisterinpitäjä ei saisi kieltäytyä, varsinkin jos lisätiedot tukevat rekisteröidyn oikeuksia. Rekisteröidyn tunnistukseen tulisi sisällyttää digitaalinen tunnistaminen, esim. pankkitunnuksilla kirjautuminen [2, kohta 57.]

Rekisteröidylle tai yleisölle tarkoitetut tiedot pitää olla tiiviisti esitettynä ja helposti saatavilla sekä ymmärrettäviä. Kyseiset tiedot tulee ilmaista yksinkertaisella ja selkeällä kielellä, tarvittaessa myös havainnollistettava. Yleisölle tarkoitettuja tietoja voi antaa sähköisessä muodossa, esim. internetsivustolla. Erityisesti lapsia koskevassa tiedotuksessa tulee käyttää niin yksinkertaista ja selkeää kieltä, että lapsikin ymmärtää sen [2, kohta 58.]

2.2 Rekisteröidyn oikeudet

Rekisterinpitäjän pitäisi tarjota rekisteröidylle keinot, joilla rekisteröity voi muokata henkilötietojaan, pyytää tietoihin muutosta tai tietojen poistamista. Keinojen pitäisi olla mahdollisuuksien mukaan ilmaisia rekisteröidylle [2, kohta 59.]

Rekisteröidyllä on oltava oikeus nähdä henkilötiedot, jotka hänestä on kerätty, jotta hän pysyy perillä henkilötietojensa käsittelyn oikeudenmukaisuudesta. Esimerkiksi rekisteröidyllä on oikeus nähdä terveystietonsa, johon on koottu diagnoosi, tutkimustulokset, lääkärien arviot ja muut hoitoa koskevat tiedot. Jos mahdollista, rekisterinpitäjän tulee tarjota suojattu etäyhteys järjestelmään, jossa rekisteröidyn henkilötiedot ovat [2, kohta 63.] Rekisterinpitäjän tulee aina erikseen tarkistaa rekisteröidyn henkilöllisyys, kun hän pyytää pääsyä tietoihin. Rekisterinpitäjä ei saa säilyttää henkilötietoja erikseen vain edellä mainittuja tapauksia varten [2, kohta 64.]

Luonnollisella henkilöllä on oikeus saada oikaistua virheelliset, häntä koskevat henkilötiedot sekä oikeus tulla unohdetuksi. Rekisteröidyn erityisoikeus on, että hänen henkilötietonsa poistetaan, kun tietoja ei enää käsitellä siihen tarkoitukseen, mihin tiedot alun perin kerättiin. Kyseisiä tietoja ei saisi myöskään käsitellä, kun niitä ei enää tarvita. Rekisteröity voi perua suostumuksensa tietojensa käsittelyyn tai vastustaa tietojensa käsittelyä. Jos rekisteröity on antanut suostumuksen tietojensa käsittelyyn lapsena, hänellä on oikeus saada tiedot poistettua [2, kohta 65.]

Kun rekisteröity on ilmoittanut, että hän haluaa kaikki tietonsa rekisteristä poistetuksi, kyseisen rekisterin rekisterinpitäjä on velvollinen ilmoittamaan muille kyseisiä henkilötietoja käsitteleville rekisterinpitäjille, että tiedot on poistettava rekisteristä, mukaan lukien tietoihin liittyvät linkit, jäljennökset ja kopiot [2, kohta 66].

2.3 Henkilötietojen suojaus

Rekisterinpitäjän pitää suojata käsittelemiensä henkilötietojen turvallisuus käyttäen asianmukaisia teknisiä toimenpiteitä. Toimenpiteiden, jotka rekisterinpitäjä päättää toteuttaa, on vastattava oletusarvoisia tietosuojaperiaatteita. Tallaisia toimenpiteitä ovat esimerkiksi henkilötietojen käsittelyn minimointi, rekisteröidyn mahdollisuus valvoa tietojensa käsittelyä ja henkilötietojen käsittelyn läpinäkyvyys [2, kohta 78.]

Rekisterinpitäjien ja henkilötietojen käsittelijöiden on tehtävä yhteistyötä valvontaviranomaisten kanssa. Viranomaisille tulee pyydettäessä esittää jotakin käsittelyä koskevat henkilötietorekisterit, jotta viranomainen voi seurata tietojenkäsittelyä rekisterin pohjalta [2, kohta 82.]

Henkilötietojen käsittelijän tai rekisterinpitäjän on arvioitava, millaisia riskejä liittyy henkilötietojen käsittelyyn ja kuinka kyseisiä riskejä voidaan lieventää. Riskien lieventämistoimenpiteillä varmistetaan asianmukainen turvallisuustaso. Tietosuojariskejä mietittäessä on otettava myös huomioon henkilötietojen käsittelyyn liittyvät riskit, esimerkiksi henkilötietojen tahallinen tai vahingossa tapahtuva tuhoaminen ja luvaton pääsy henkilötietoihin [2, kohta 83.]

Yksi esimerkki huonosta henkilötietojen suojauksesta on Liiketoimintasuunnitelma.com-sivustolle huhtikuussa 2018 tapahtunut tietomurto, jonka seurauksena 130 000

käyttäjätunnusta ja salasanaa varastettiin. Kyseinen tietomurto on yksi vakavimmista Suomessa tapahtuneista tietomurroista [9.]

2.4 Tietoturvaloukkaus

Tietoturvaloukkaukseen, joka kohdistuu henkilötietoihin, pitää puuttua nopeasti ja tehokkaasti, ettei siitä aiheudu fyysisiä, aineellisia tai aineettomia vahinkoja luonnolliselle henkilölle, esim. luonnollisen henkilön identiteetin varastaminen. Mahdollisesta tietoturvaloukkauksesta on ilmoitettava viranomaiselle 72 tunnin kuluessa tietoturvaloukkauksen huomaamisesta. Jos ilmoitusta ei voida tehdä 72 tunnin kuluessa, ilmoitukseen liitetään syy viivästyksestä [2, kohta 85.]

Tietoturvaloukkauksesta on hyvä myös ilmoittaa rekisterissä oleville rekisteröidyille, että heidän tietonsa voivat olla vaarassa, ilmoitus tehdään mahdollisimman nopeasti. Rekisteröidyn ilmoituksessa kuvataan tietoturvaloukkauksen luonne ja esitetään suosituksia, kuinka rekisteröity voi lieventää loukkauksen mahdollisia haittavaikutuksia. [2, kohta 86] Rekisterinpitäjät tarkistavat tietoturvaloukkauksen sattuessa, onko kaikki asianmukaiset suojatoimenpiteet toteutettu. Tämä auttaa selvittämään tietoturvaloukkauksen vakavuutta [2, kohta 87.]

3 Valmistautuminen

Euroopan unionin uusi tietosuoja-asetus koskee kaikkia yrityksiä, jotka käsittelevät henkilötietoja toiminnassaan. Asetusta sovelletaan henkilötietojen käsittelyn tarpeen mukaan.

Yrityksen on hyvä aluksi selvittää, millaisella tasolla henkilötietojen käsittely on, millaisia henkilötietoja yrityksellä on hallussaan, mihin tarkoitukseen henkilötietoja kerätään tai käytetään, kuinka suojaustoimenpiteet on toteutettu ja mikä on tietoturvan laita. Tyypillisimpiä yrityksen hallussa olevia henkilötietoja ovat asiakkaan nimi, osoitteet, puhelinnumero ja sähköpostiosoitteet. Selvitystä kutsutaan tietotilinpäätökseksi. Henkilötietojen käsittelyn nykytilan selvittämisen jälkeen kartoitetaan konkreettiset muutokset ja toimenpiteet [1, sivu 11.]

3.1 Tietotilinpäätös

Tietotilinpäätöksellä saadaan yrityksen tietojenkäsittelyn nykytilasta kokonaiskuva sekä arvio yrityksen tietosuojasta ja tietoturvasta. Tietotilinpäätöksen sisältö kuvaa esimerkiksi seuraavia asioita: [7.]

Mitä tietovarantoja yrityksellä on hallussa

- Ohjelmat ja tietojärjestelmät joissa käsitellään yrityksen keräämiä tietoja.

Mikä on yrityksen tietoarkkitehtuuri

- Millaisia ohjelmia ja tietojärjestelmiä yritykseltä löytyy ja miten tieto liikkuu niiden välillä.

Mikä on yrityksen hallussa olevien tietojen laatu ja käytettävyys.

- Mihin kerättyjä tietoja käytetään ja millaista tietoa se on.

Mitä menettelytapoja ja periaatteita yritys noudattaa tietojen käsittelyssä

- Onko yrityksen henkilökunnalla riittävästi tietoa käsiteltävien tietojen julkisuudesta, salassa pidosta ja niiden suojaamisesta.

Miten tiedot on suojattu.

- Millaisia fyysisiä ja tietoteknisiä ratkaisuja käytetään tietojen suojaukseen.

Miten tietojen käyttöä valvotaan.

- Ketkä pääsevät käsiksi tietoihin.

Miten toteutetaan rekisteröityjen oikeudet tietojen käsittelyssä

- Pääsevätkö rekisteröidyt tarkastelemaan ja muokkaamaan omia tietojaan.

3.2 Tietosuojaperiaatteet

Yrityksen on henkilötietojensa käsittelyssä noudatettava tietosuojaperiaatteita, periaatteet auttavat rekisterinpitäjää käsittelemään tietoja rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla. Tietosuojaperiaatteita ovat:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus [1, sivu 12.]

Näitä periaatteita tulee noudattaa henkilötietojen käsittelyn kaikissa vaiheissa, rekisterinpitäjä vastaa siitä, että periaatteita noudatetaan ja rekisterinpitäjän on myös pystyttävä osoittamaan se [1, sivu 12.]

3.3 Osoitusvelvollisuus

Osoitusvelvollisuus edellyttää, että henkilötietojen käsittely prosessien ja tietosuojaperiaatteiden toteutus on dokumentoitu huolella. Yritykset voivat käyttää tietosuoja sertifikaatteja, jotka ovat tietosuoja-asetuksen mukaisia, osoittaakseen, että periaatteita noudatetaan. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on pidettävä selostetta (dokumenttia) käsittelytoimista, joista he ovat vastuussa. Selosteesta varmistetaan, että toimet noudattavat asetusta. Seloste tulee pyydettäessä näyttää viranomaisille ja selosteen on oltava kirjallisessa muodossa [1, sivu 14.]

Tietoturvaloukkauksen sattuessa, yrityksen pitää pystyä osoittamaan, että tietoturvaloukkaus on tapahtunut. Tämä tapahtuu käyttämällä järjestelmää, jolla voidaan monitoroida yrityksen verkkoliikennettä, esim. SIEM-järjestelmä (Security Information and Event Management). SIEM-järjestelmällä yritys voi myös huomata tietoturvaloukkauksen

ajoissa ja yrittää rajoittaa mahdolliset haitat minimiin [4.] On parempi huomata tietoturvaloukkaus itse, kuin lukea siitä päivän lehdestä. Huomaamatta jäänyt tietoturvaloukkaus vaikuttaa suuresti yrityksen maineeseen.

3.4 Tietosuojavastaavan nimittäminen

Yrityksen tulee nimittää henkilöstöstään yksi henkilö, joka toimii tietosuojavastaavana. Nimitysvelvollisuus koskee kaikkia viranomais- ja julkisenhallinnon elimiä sekä sellaisia yrityksiä, jotka käsittelevät laajamittaisiesti henkilötietoja toiminnassaan. Tietosuoja-asetuksessa laajamittaista käsittelyä ei ole erikseen määritelty, mutta jos yritys käsittelee henkilötietoja sen verran, jotta niiden joutuminen vääriin käsiin aiheuttaa vahinkoa rekisteröidyille, käsittelyä voidaan pitää laajamittaisena [5, kohta 2.1 ja 2.1.3.] Rekisteröidylle aiheutuva vahinko voi olla esimerkiksi henkilöllisyyden varastaminen tai rekisteröidyn tiedoilla tehdään tilauksia verkkokaupoista.

Jos yritykselle ei ole selvää, pitääkö sen nimittää tietosuojavastaava, tulee yrityksen tehdä selvitys tietosuojavastaavan nimittämisestä ja dokumentoida se. Dokumentaatiolla yritys pystyy osoittamaan, että se on ottanut olennaiset tekijät tietosuojavastaavan nimittämisessä huomioon [5, kohta 2.1.] Tietosuojavastaavana voi toimia yrittäjä itse, jos kysymyksessä on mikroyritys ja henkilötietoja käsitellään vain yrityksen omaan toimintaan liittyen, esimerkiksi yritys harjoittaa myyntiä ja kerää vain siihen tarvittavia tietoja. Jos yrityksen toiminnassa halutaan ruveta käsittelemän laajemmin henkilötietoja, yrittäjän on hankittava siihen liittyvää tietotaitoa tai selvittää, voiko tietosuojavaltuutetun toimia ulkoistaa [8.]

Tietosuojavastaavan tehtävinä on antaa neuvoja ja tietoja rekisterinpitäjälle tai henkilötietojen käsittelijälle koskien tietosuoja-asetuksen mukaisia velvollisuuksia. Tietosuojavastaava valvoo, että yrityksessä noudatetaan tietosuoja-asetusta sekä pyydettäessä antaa neuvoja tietosuojan vaikutusarvioinnista. Viranomaisten kanssa tietosuojavastaavan on tehtävä yhteistyötä, ja vastaava myös toimii yhteyshenkilönä viranomaisille [2, 39 artikla.]

3.5 Sanktiot

Tietosuoja-asetus tuli voimaan 25. toukokuuta 2018, jonka jälkeen tietosuojan tulee olla toteutettu asetuksen määrittelemällä tavalla. Jos näin ei kumminkaan ole ja tarkastuksissa huomataan puutteita tietosuojassa, seuraa siitä sanktio. Sanktioista määrää kansallinen valvontaviranomainen.

Lievimmillään sanktio voi olla varoitus tai huomautus. Kovempi sanktio on, että yritys joutuu keskeyttämään kokonaan tietojenkäsittelyn, kunnes tarvittavat korjaukset tietosuojaan ja tietojenkäsittelyyn liittyen on tehty. Kovin sanktio on sakko, joka on joko enimmillään 20 miljoonaa euroa tai 4 % yrityksen vuosittaisesta kokonaisliikevaihdosta. Sakosta määrätään se, kumpi johtaa suurempaan summaan [3.] Pienille yrityksille sakon maksimisumma on sama. Käytännössä sakon lopullinen summa määräytyy aiheutuneen vahingon mukaan, esimerkiksi menetettyjen henkilötietojen määrä vaikuttaa sakon suuruuteen [8.]

4 Pienyrittäjän näkökulma

EU:n tietosuoja-asetus koskee kaikkia yrityksiä, jotka käsittelevät toiminnassaan henkilötietoja ja pitävät niistä rekisteriä. Moni pk-yritys ei todennäköisesti ole tehnyt juurikaan mitään tietosuoja-asetuksen eteen. Pk-yrityksen kannattaa ensiksi selvittää, millaisia henkilötietoja yrityksessä käsitellään ja missä niitä säilytetään, eli selvitettävä yrityksen hallussa olevien henkilötietojen käsittelyn nykytila. Näitten tietojen perusteella lähdetään selvittämään tietosuoja-asetuksen toteutusta.

Yrityksen on selvitettävä, tarvitseeko sen nimittää tietosuojavastaavaa yritykseen vai riittäkö, että yritys nimittää yhden työntekijöistään vastaamaan tietosuoja-asetukseen liittyvistä asioista. Kyseinen henkilö ei kuitenkaan ole tietosuojavastaava, mutta voi tietyin ehdoin toimia virallisena tietosuojavastaavana [5, sivu 6, Tietosuojavastaavan nimittäminen.] Tietosuojavastaavan tarve riippuu siitä, millaista tietoa ja kuinka paljon kyseistä tietoa yritys kerää ja siitä, käsitteleekö yritys pääasiallisesti henkilötietoja liiketoiminnassaan [3].

Kerätyistä henkilötiedoista yrityksen on pidettävä rekisteriä, tietoja käsitellään säännöllisesti, jos kerätyt tiedot uhkaavat ihmisten oikeuksia ja vapauksia tai jos kerätyt tiedot ovat arkaluontoisia tai rikosrekisteritietoja. Rekisteriin kirjataan:

- yrityksen nimi ja yhteistiedot
- tietojenkäsittelyn syy
- rekisteröityjen ryhmien ja henkilötietojen kuvaus
- tietoja vastaanottavien organisaatioiden ryhmät
- tietojen siirtäminen toiseen maahan tai organisaation
- tietojen poistamisen määräaika, jos mahdollista
- kuvaus tietojenkäsittelyn yhteydessä käytettävistä turvatoimista, jos mahdollista [3.]

Tietojärjestelmiin pk-yritys joutuu tekemään muutoksia, uudistamaan olemassa olevia ohjelmia tai päivittämään ohjelmat uusimpiin versioihinsa, jotta niiden tietoturva on ajan tasalla. Tietoturvaa ja tietojärjestelmiä uudistamalla taataan tietojenkäsittelyn suojaus, tietojen keräämisestä tietojen tuhoamiseen [1, kohta 9. Tietoturva.] Tietojärjestelmiin liittyvät sopimukset on päivitettävä tietosuoja-asetuksen mukaisiksi, esimerkiksi rekisterinpitäjän ja henkilötietojenkäsittelijän välisessä sopimuksessa on kirjattuna, kuinka henkilötietojenkäsittelijä käsittelee rekisterinpitäjän käyttämiä henkilötietoja. Kaksi vuotta ja sitä vanhemmat sopimukset pitää uusia, kun niissä ei ole uuden tietosuoja-asetuksen mukaisia asioita otettu huomioon [1.]

Yrityksen henkilökuntaa on hyvä kouluttaa tietosuoja-asetuksesta, jotta henkilökunta tietäisi miten asiakkaiden henkilötietoja pitää käsitellä ja millaisia oikeuksia asiakkaalla on henkilötietietojensa suhteen, siltä varalta, että asiakas tulee kyselemään millaisia tietoja hänestä on yrityksellä. Asiakkaille on hyvä myös tiedottaa, millaisia oikeuksia heillä on tietojensa suhteen.

5 Yritys-case

Opinnäytetyön toimeksiantaja järjesti tarkasteltavaksi yritykseksi lomamökkiä vuokraavan Vaarinkallion. Vaarinkallio ei ole varsinaisesti yritys, vaan yksityishenkilö vuokraa omaa mökkiään.

Tietosuoja-asetuksessa sanotaan, miten asetusta sovelletaan yksityishenkilöön:

> Tätä asetusta ei sovelleta henkilötietojen käsittelyyn,
>
> jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa [2, 2. artikla, kohta 2, sivut 108-109.]

Näin ollen tietosuoja-asetus ei koske Vaarinkalliota, mutta mitä Vaarinkallion tulisi tehdä, jos toiminta muutettaisiin yksityishenkilöstä yritykseksi? Vaarinkalliolla on muutama kymmenen asiakasta vuodessa.

5.1 Yritykseksi muuttuminen

Toimintansa yritykseksi muuttamisessa Vaarinkallion olisi ensiksi selvitettävä henkilötietojen käsittelyn nykytila, miten käsitellään ja kuka tai ketkä käsittelevät. Nykytilan selvityksen apuna voi käyttää valtionvarainministeriön Vahti-työryhmän Tietosuojan tukityökalua, jonka voi ladata työryhmän sivuilta [11.] Tukityökalulla on helppo hahmottaa rekisterinpitäjän velvollisuudet, rekisteröidyn oikeudet sekä tarvittavat toimenpiteet.

Vaarinkallio ei pidä asiakkaistaan varsinaista rekisteriä missään. Kun asiakas tekee varauksen mökistä, häneltä kysytään yhteystiedot laskua varten, tiedot kirjataan väliaikaisesti paperilapulle. Jos yrityksessä toimittaisiin näin, täyttäisi se tietosuoja-asetuksen vaatimuksen henkilötietojen lyhyestä säilytysajasta, kunhan paperilappu hävitettäisiin oikeaoppisesti, kun sillä olevia henkilötietoja ei enää tarvita.

Vaihtoehtoisesti asiakas voi lähettää yhteystietonsa tekstiviestillä, toisaalta, jos asiakkaan henkilötietoja sisältäviä tekstiviestejä ei poisteta puhelimesta, voidaan sitä pitää henkilötietorekisterinä. Laskun Vaarinkallio tekee heti ja lähettää laskun asiakkaalle. Laskun tekoon Vaarinkallio käyttää toiselta yritykseltä ostamaansa, nettiselaimessa toimivaa laskutuspalvelua. Palvelua käytetään tavalliselta tietokoneelta (pöytä- tai kannettava tietokone).

5.2 Tietojenkäsittely

Asiakkaiden tietojenkäsittely kannattaisi muuttaa paperisesta sähköiseen, mikä helpottaisi käsittelyä, kun tietoja ei ole usealla eri paperilla vaan kaikki tiedot olisivat yhdessä paikassa, esimerkiksi Excel-tiedostossa. Paperisena säilytettäviä henkilötietoja voidaan pitää myös rekisterinä, jota pitäisi käyttää tietosuoja-asetuksen mukaisesti. Asiakkaan henkilötietoja sisältävä paperi tulisi hävittää, kun kyseisiä tietoja ei enää tarvita. Puhelimessa olevat tekstiviestit, jotka sisältävät asiakkaan henkilötietoja, pitäisi myös poistaa, kun tiedot on joko kirjattu paperiseen tai sähköiseen järjestelmään ja kyseinen tekstiviesti poistaa puhelimesta.

Paperinen käsittely tietysti poistaa tietomurron uhkan melkein kokonaan, voihan joku siltikin murtautua asuntoon, jossa papereita säilytetään. Asiakastietoja sisältäviä papereitakin pitäisi pitää suojatussa paikassa, esimerkiksi kassakaapissa tai muussa lukittavissa olevassa paikassa.

Sähköisessä muodossa olevaa asiakastietoa pitää säilyttää vain paikallisesti, tiedostoa ei tallenneta pilvitallennuspalveluihin ja siitä on hyvä pitää varmuuskopiota parissakin eri paikassa, esimerkiksi ulkoisilla kiintolevyillä. Kyseiset kiintolevyt on hyvä myös pitää lukkojen takana.

5.3 Tietosuojavastaava

Nykytilan selvittämisen jälkeen on selvitettävä, tarvitseeko Vaarinkallio tietosuojavastaavaa. Tietosuoja-asetus sanoo, että tietosuojavastaava pitää olla, jos yritys käsittele pääasiallisesti toiminnassaan henkilötietoja. Tietosuojavastaavan nimittämisestä on tehtävä selvitys, miksi tarvitaan tai miksi ei tarvita.

Vaarinkallio vuokraa lomamökkiä, joten he käsittelevät toiminnassaan paljon asiakkaiden yhteystietoja, joten Vaarinkallion olisi nimitettävä tietosuojavastaava. Tietosuojavastaavana voi toimia yksi yrityksen työntekijöistä, joka on hyvin perillä yrityksen tietojärjestelmistä. Kyseinen henkilö ei kumminkaan saa olla yrityksessä päättävässä asemassa. Yksi vaihtoehto tietosuojavastaavan tehtävistä on niiden ulkoistaminen, jolloin tietosuojavastaava hankitaan yrityksen ulkopuolelta. Ulkoistamalla yrityksestä ei tarvitse sitoa yhtä henkilöä tietosuojavastaavan tehtäviin, millä voi olla merkitystä yrityksen toimintaan. Tietosuojavastaavan palveluita tarjoaa esimerkiksi Privaon [12].

5.4 Tietojärjestelmät

Tietotekniikkaan Vaarinkallion ei tarvitsisi ainakaan alkuun investoida oikeastaan ollenkaan, yrityksen toiminta vaadi palvelinjärjestelmää tai vain tiettyä tarkoitusta varten tehtyjä erikoisohjelmistoja, muuta kuin laskutuspalvelun, joka toimii nettiselaimessa. Tietokoneeksi, jolla käsitellään asiakkaitten tietoja, riittää tavallinen pöytä- tai kannettava tietokone.

Kyseisellä tietokoneella on pidettävä tietoturva ajan tasalla, haittaohjelmien torjuntaohjelmaksi soveltuu ihan kuluttajille tarkoitettu tietoturvaohjelmisto, esim. F-secure. Reitittimeksi soveltuu myös kuluttajille tarkoitettu malli. Reitittimestä on hyvä muuttaa oletussalasana joksikin toiseksi sekä piilottaa reitittimen nimi, jotta reitittimen hakkerointi olisi vaikeampaa mahdollisille verkkorikollisille.

Mahdollisista tietojärjestelmäinvestoinneista Vaarinkallion pitää investoida ainakin tietoturvaan, tietoturvan päivitykset tietokoneilla, jolla mahdollisesti käsitellään asiakkaiden henkilötietoja. Kuluttajille tarkoitettu viruksen torjunta ja palomuuriohjelmisto on alkuun riittävä tietoturva, mutta ne kannattaa kuitenkin vaihtaa yrityksille tarkoitettuihin versioihin.

5.5 Tulevaisuus

Tulevaisuudessa Vaarinkallion keräämien henkilötietojen laatu todennäköisesti ei tule muuttumaan, edelleen kerätään asiakkaan nimi, osoite ja puhelinnumero laskutusta varten. Tiedot kysyttäisiin asiakkaalta varauksen teon yhteydessä. Ulkopuolisten tahojen kanssa pitäisi tehdä sopimukset Vaarinkallion keräämien henkilötietojen mahdollisesta käsittelystä, esimerkiksi tilitoimiston kanssa on tehtävä sopimus henkilötietojen käsittelystä. Sopimuksella varmistetaan, että ulkopuolinen taho käsittelee Vaarinkallion lähettämiä tietoja tietosuoja-asetuksen mukaisesti.

Vaarinkallio voi tulevaisuudessa hyödyntää Hotels.comin kaltaista varauspalvelua tai omille verkkosivuilleen lisätä varauslomakkeen. Varauslomakkeessa on tultava asiakkaalle selvästi esille, mitä tietoja hänestä kerätään, kun hän tekee varauksen ja miksi kyseiset tiedot kerätään. Jo olemassa olevan varauspalvelun kanssa on myös tehtävä sopimus henkilötietojen käsittelystä, varauspalveluhan tallentaa asiakkaan tekemän varauksen ja lähettää siitä tiedot Vaarinkalliolle.

Palvelimeen investointia en suosittelisi ainakaan alkuvaiheessa, tehokas työasema on riittävä Vaarinkallion kokoisessa yrityksessä. Jos Vaarinkallion toiminta kasvaisi tulevaisuudessa huomattavasti, enemmän asiakkaita ja useampi vuokramökki, silloin kannattaisi investoida palvelimeen, joko fyysiseen tai pilvipalvelimeen. Pilvipalvelimen hankkimisessa on otettava huomioon missä maassa itse vuokrattavan pilven palvelimet sijaitsevat. Ihanteellisessa tilanteessa palvelimet sijaitsisivat Euroopan sisällä.

Palvelimella säilytettäisiin yrityksen liiketoimintaan liittyviä asiakirjoja, asiakastietoja ja muuta yritykselle tärkeää tietoa sekä käytettäisiin yrityksen tarvitsemia ohjelmistoja. Tietokehittämiskeskus Ry:n (TIEKE) nettisivuilta löytyy lisäohjeistusta palvelimen hankkimiseen [13].

6 Yhteenveto

Nykyisessä toimintamuodossaan Vaarinkalliota eivät koske uuden tietosuoja-asetuksen tuomat uudistukset henkilötietojen käsittelyyn. Vaarinkallion kannattaisi miettiä valmiiksi toimenpiteitä, joita tarvitaan, jos toimintamuoto muutetaan yritykseksi. Yritykseksi muuttuminen ei Vaarinkallion tapauksessa vaatisi hirveästi työtä teknisesti, kun ei tarvitsisi investoida juurikaan tietotekniikkaan. Tietosuojavastaavan nimittäminen ja sopimuksien teot tilitoimiston ja mahdollisten yhteistyökumppaneiden kanssa ovat todennäköisesti eniten työtä aiheuttavia toimia.

7 Pohdintaa

Tietosuoja-asetusta uudistamalla EU haluaa yhtenäistää henkilötietojen käsittelyä koko unionin alueelle, asetuksen soveltaminen alkoi 25.5.2018. Onko asetuksesta sitten mitään hyötyä, vai onko sen vain tarkoitus aiheuttaa ylimääräistä työtä yrityksille?

Työtähän asetus aiheuttaa yrityksille, millään yrityksellä tuskin on tietosuoja asiat asetuksen määräämällä tavalla. Yrityksien olisi muutenkin hyvä tarkistaa parin vuoden välein tietosuojan laita. Hyötyä asetuksesta on koko unionin alueella. Kun jokaisessa unionin maassa yritykset käsittelevät henkilötietoja samalla tavalla, on helpompaa valvoa asetuksen noudattamista.

Yrityksille asetuksesta on paljonkin hyötyä. Tietoturvan taso yrityksessä paranee, kun asetus edellyttää kunnollista tietoturvaa. Henkilötietojen käsittely yrityksessä yhtenäistyy, kun eri tietojärjestelmissä olevat tiedot kootaan yhteen paikkaan. Samalla poistuvat myös turhat henkilötietorekisterit sekä turhat tiedot rekistereistä, esimerkiksi henkilön, joka ei ole enää asiakkaana yrityksessä, tiedot poistuvat. Tietojenkäsittelyn parantumisen myötä myös liiketoiminta paranee. Asiakaspalvelu paranee, kun asiakkaan vaatimuksiin osataan vastata paremmin paremman tiedonkäsittelyn myötä, myös johdon ja työntekijöiden välinen kommunikointi paranee.

Tietosuoja-asetuksen voimaantulo voi olla verkkorikollisille otollinen aika koittaa kiristää yrityksiä henkilötietoja varastamalla, kun yrityksessä ei olla parannettu tietoturvan tasoa, vaikka asetus sitä edellyttää. Tietomurtojen, tai ainakin tietomurtojen yritysten, määrä todennäköisesti vähän kasvaa seuraavan vuoden aikana, kun verkkorikolliset koittavat murtautua yrityksiin. Suurimmassa vaarassa ovat yritykset, jotka eivät ole huolehtineet tietosuoja-asetuksen toteuttamisesta.

Tietosuoja-asetuksesta seuraa siis sekä hyvää että pahaa. Asetuksen toteuttaminen edellyttää paljon työtä, jota on vain tehtävä, koska asetus määrää, muuten yritykselle voi tulla isot sakot.

Lähteet

1 Tietosuojavaltuutetun toimisto. Miten valmistautua EU:n tietosuoja-asetukseen. 2017. Verkkodokumentti. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. 31.1.2018.

2 Euroopan Parlamentin ja Neuvoston Asetus (EU) 2016/679. 15.1.2018.

3 Tietosuojavaltuutetun toimisto. Tietosuoja-asetuksen vaikutukset pk-yrityksille. 2017. Verkkodokumentti. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/z0PdCBWW7/Data_protection_infographic_FI-LR.pdf. 3.3.2018.

4 Viestintävirasto. SIEM lokitiedon hyödyntämisessä, 2016. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603151527.html. 10.3.2018.

5 Tietosuojavaltuutetun toimisto. Tietosuojaryhmä. Tietosuojavastaavat. 2017. Verkkodokumentti. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/UvreCmOiN/Tietosuojavastaavia_koskevat_ohjeet_wp243rev01_fi.pdf. 16.3.2018.

6 Vaarinkallio. Hirsihuvila Kolilla. https://vaarinkallio.com/en/. 20.3.2018.

7 Tietosuojavaltuutetun toimisto. Laadi Tietotilinpäätös. 24.4.2012. Verkkodokumentti. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf.

8 Karelia AMK. KoDa Hanke. GDPR – Webinaari. 28.2.2018. http://www.karelia.fi/koda/tyokalut-2/julkaisut/. 5.4.2018.

9 Viestintävirasto. Kyberturvallisuus. Tietoturva nyt! 6.4.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/04/ttn201804061405.html. 15.4.2018.

10 Tietosuojavaltuutetun toimisto. Tietosuojavaltuutettu. http://www.tietosuoja.fi. 5.2.2018.

11 Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto. Excel työkalu. https://www.vahtiohje.fi. 2.4.2018.

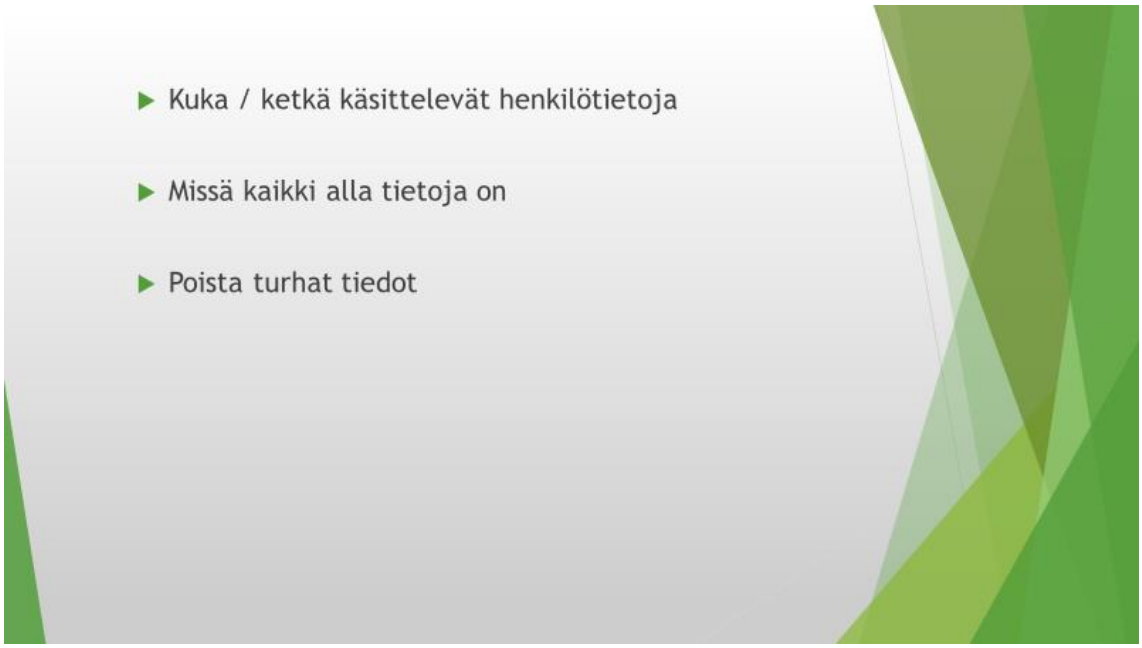
12 Privaon. Tietosuojavastaavan ulkoistaminen. https://privaon.fi/palvelut/tietosuoja-vastaava/. 9.4.2018

13 Tietokehittämiskeskus RY. Tietotekniikkahankinnat. Valitsenko työaseman vai palvelimen? https://www.tieke.fi/pages/viewpage.action?pageId=3441272. 10.4.2018

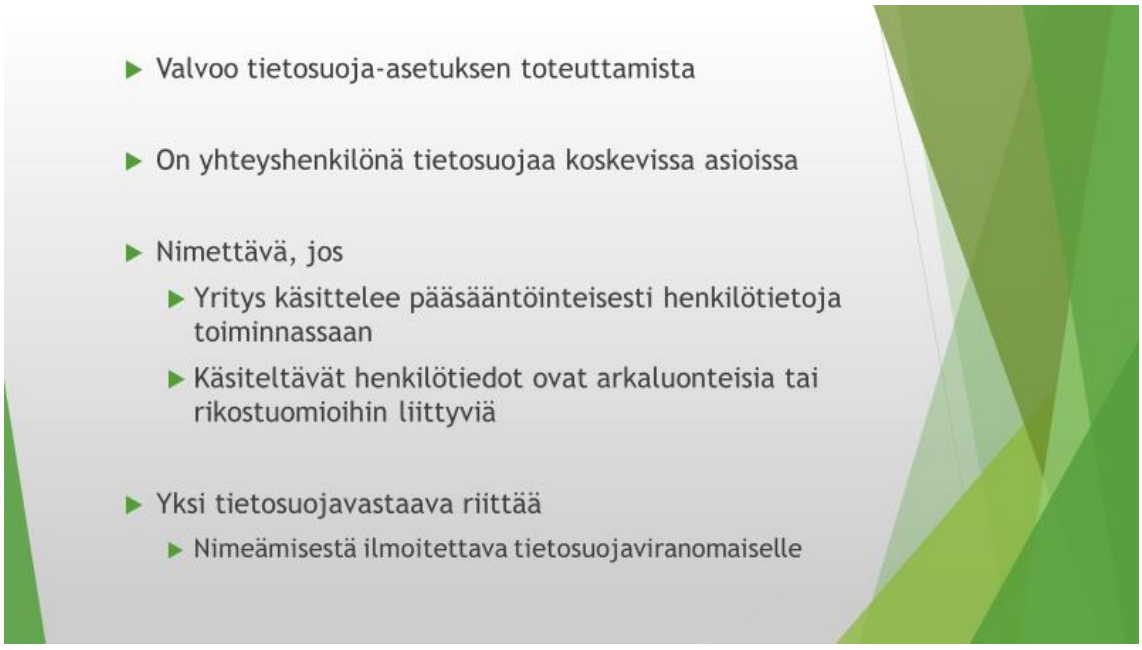
Liitteet

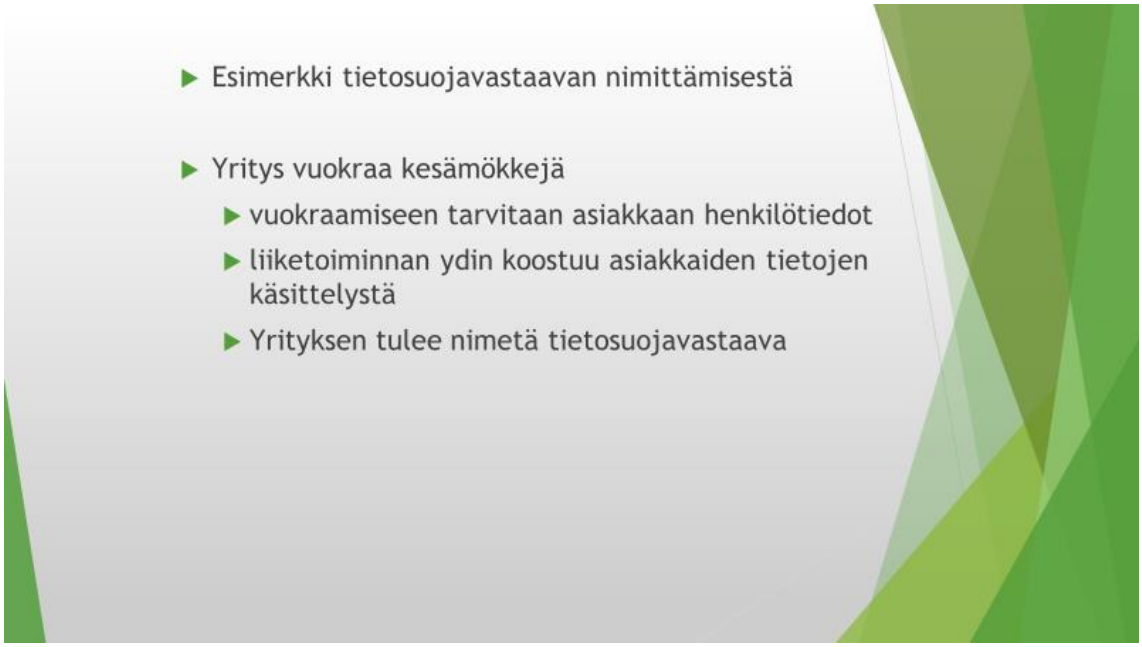
EU:n tietosuoja-asetus


Selvitä nykytila

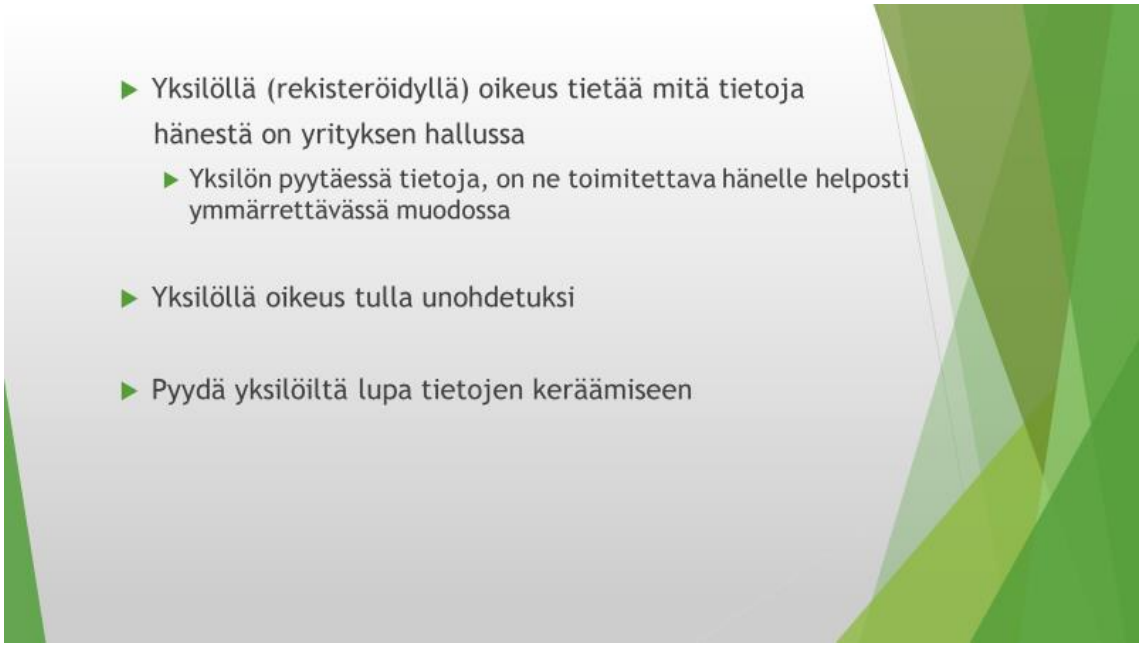

Kuka / ketkä käsittelevät henkilötietoja
Missä kaikki alla tietoja on
Poista turhat tiedot


Nimeä tietosuojavastaava

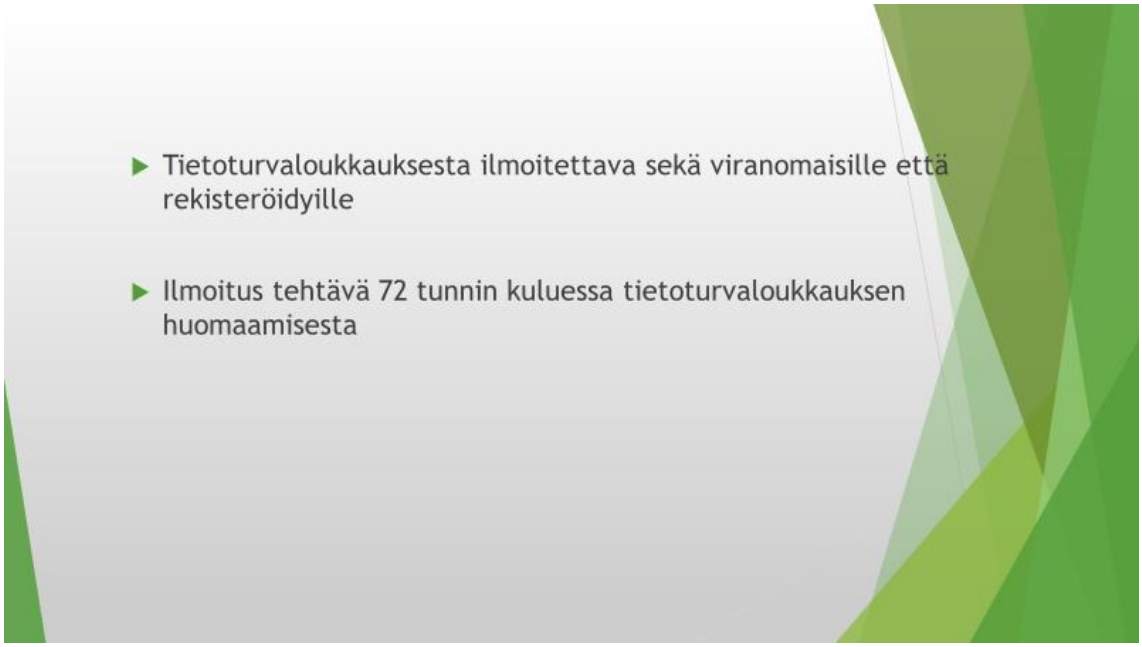

Valvoo tietosuoja-asetuksen toteuttamista
On yhteyshenkilönä tietosuojaa koskevissa asioissa
Nimettävä, jos
Yritys käsittelee pääsääntöinteisesti henkilötietoja toiminnassaan
Käsiteltävät henkilötiedot ovat arkaluonteisia tai rikostuomioihin liittyviä
Yksi tietosuojavastaava riittää
Nimeämisestä ilmoitettava tietosuojaviranomaiselle


Esimerkki tietosuojavastaavan nimittämisestä
Yritys vuokraa kesämökkejä
vuokraamiseen tarvitaan asiakkaan henkilötiedot
liiketoiminnan ydin koostuu asiakkaiden tietojen käsittelystä
Yrityksen tulee nimetä tietosuojavastaava

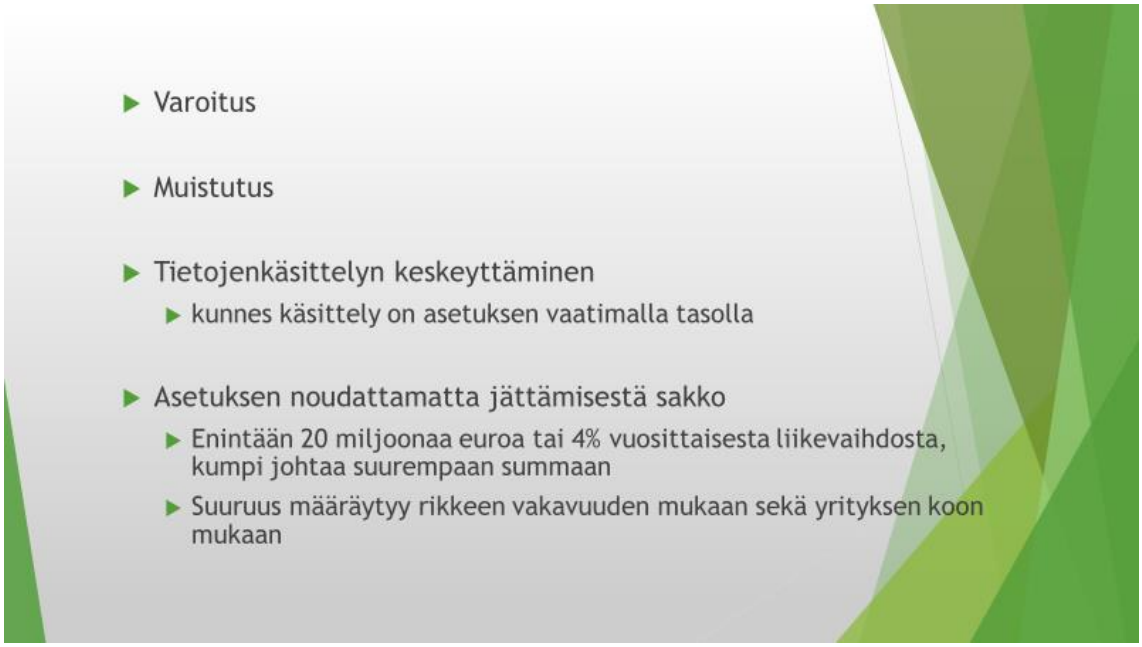

Yksilön oikeudet

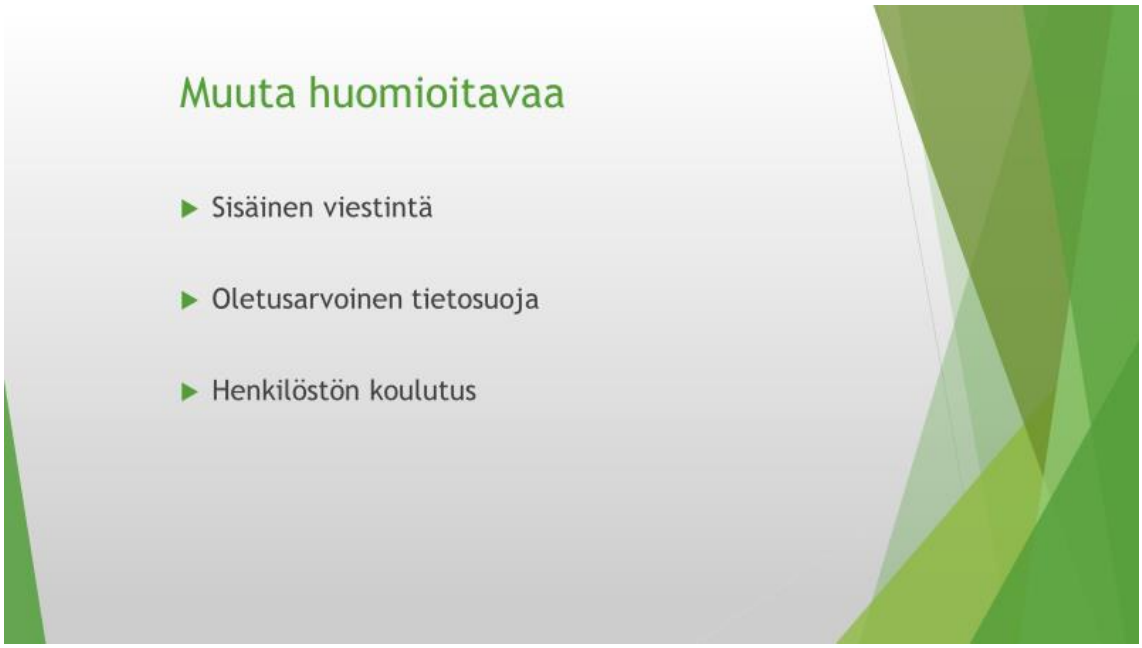

Yksilöllä (rekisteröidyllä) oikeus tietää mitä tietoja hänestä on yrityksen hallussa
Yksilön pyytäessä tietoja, on ne toimitettava hänelle helposti ymmärrettävässä muodossa
Yksilöllä oikeus tulla unohdetuksi
Pyydä yksilöiltä lupa tietojen keräämiseen


Ilmoitusvelvollisuus


Tietoturvaloukkauksesta ilmoitettava sekä viranomaisille että rekisteröidyille
Ilmoitus tehtävä 72 tunnin kuluessa tietoturvaloukkauksen huomaamisesta


Sanktiot


Varoitus
Muistutus
Tietojenkäsittelyn keskeyttäminen
kunnes käsittely on asetuksen vaatimalla tasolla
Asetuksen noudattamatta jättämisestä sakko
Enintään 20 miljoonaa euroa tai 4% vuosittaisesta liikevaihdosta, kumpi johtaa suurempaan summaan
Suuruus määräytyy rikkeen vakavuuden mukaan sekä yrityksen koon mukaan


Muuta huomioitavaa
Sisäinen viestintä
Oletusarvoinen tietosuoja
Henkilöstön koulutus