opsec

Tietosuojaopas pienille yrityksille

Helmikuu 2019

Suomen Yrittäjäopisto

Euroopan maaseudun kehittämisen maatalousrahasto: Eurooppa investoi maaseutualueisiin

MAASEUTU 2020

Elinkeino-, liikenne- ja ympäristökeskus

1. Johdanto 3
2. Alkuun 4
3. Henkilötietojen kartoittaminen 6
4. Henkilötietojen käsittelyn tarkoitusten ja lainmukaisuuden selvittäminen 10
5. Riskienhallinta 15
6. Tietojen siirrot ja sopimukset käsittelijöiden kanssa 19
7. Rekisteröityjen oikeudet 23
8. Rekisteröidyille informointi 26
9. Poikkeamien hallinta ja ilmoitusvelvollisuus 30
10. Nettisivut ja evästeet 33
11. Sähköpostimarkkinointi 36
12. Tietosuojavastaava 38
13. Jatkuvaa toimintaa ja laadun kehittämistä 40

1. Johdanto

Tervetuloa tutustumaan pienten yritysten tietosuojaoppaaseen. Tämän oppaan tarkoitus ei ole opettaa, mitä kaikkea EU:n tietosuoja-asetus pitää sisällään, vaan kertoa mahdollisimman konkreettisesti se, mitä pienen yrityksen on tehtävä tietosuojan toteutumisen eteen. Oppaassa ei siis keskitytä perinpohjaisesti perustelemaan, miksi asioita on tehtävä, vaan siihen, mitä pienyrittäjän on vähintään tiedettävä ja dokumentoitava omasta liiketoiminnasta tietosuojan puitteissa.

Tässä 13. osaisessa oppaassa käydään vaiheittain läpi ne toimet, jotka pienen yrityksen on vähintään tehtävä tietosuoja-asetuksen eteen. Tavoitteena on kertoa käytännön tasolla, mitä tietosuojaan liittyviä asioita on huomioitava yrityksen liiketoiminnassa. Tarkoitus on myös helpottaa yrittäjän urakkaa tietosuojatyön ja siihen liittyvän dokumentoinnin parissa.

Tietosuojaan liittyvässä toiminnassa erilaisten asioiden dokumentointi on erittäin tärkeässä roolissa. Tämä tarkoittaa, että yrityksen tietosuojaan liittyvät ohjeet ja käytännöt tulee olla kirjallisesti ylhäällä jossain siten, että voidaan myöhemmin näyttää toteen yrityksen toimivan tietosuojan kannalta oikein. Juuri dokumentointiin liittyvät vaatimukset ovat yksi suurimmista muutoksista verrattuna aiempaan lainsäädäntöön. Kun on tekemisissä esimerkiksi verottajan, työsuojelupiirin, pelastuslain tai elintarvikehygieniaan liittyvien asioiden kanssa, ilman “mustaa valkoisella” ei voi asioita todistaa. Jatkossa tätä dokumentointia tulee tehdä myös tietosuojan parissa - vaikka yrittäjästä joskus tuntuisikin siltä, ettei aika riitä kaikkien dokumenttien tekemiseen.

Oppaan liitteenä on mallilomakkeita ja -työkaluja, joihin teksteissä viitataan. Näitä dokumentteja voidaan käyttää apuna yrityksen tietosuojatyössä. Huomioitavaa on, että liiketoiminta tai yrityksessä käsiteltävät henkilötiedot saattavat edellyttää myös enemmän toimia kuin tähän oppaaseen on koottu. Sen vuoksi oppaassa on mukana *Lisätietoja -liite*, jonka avulla voi tarvittaessa tutustua tietosuoja-asetuksen vaatimuksiin tarkemmin ja saada sitä kautta lisäohjeita tietosuojatoiminnan tueksi. Oppaaseen on kerätty vain tärkeimmät tietosuoja-asetuksen velvoitteet ja kaikkein pienimmille yrityksille soveltuvat ohjeet.

Lisätietoja -liitteessä viitataan tämän oppaan osioihin ja sieltä löytyvät suorat viittaukset tietosuojalainsäädäntöön sekä erilaisiin netistä löytyviin tukimateriaaleihin. Oppaan tekstistä löytyy myös numeroidut viittaukset Lisätietoja -liitteen eri kohtiin. Esimerkiksi seuraavalta sivulta löytyy tämänkaltainen viittaus: [1.]. Tämä tarkoittaa, että Lisätietoja -liitteestä löytyy tekstin aiheeseen liittyvää informaatiota.

Oppaan osat 1.-4. tulisi käydä ensimmäisenä läpi ja siinä järjestyksessä kuin ne oppaassa ovat. Muiden osien kannalta ei ole niin tärkeää, missä järjestyksessä niitä käsittelee. Kannattaa kuitenkin palata myöhemmin tarkistamaan, ettei osista (tietosuojalainsäädännön osa-alueista) jää jokin asia huomioimatta.

2. Alkuun

Tietosuojatyötä aloittaessa kannattaa muistaa, ettei tietosuoja-asetusta sovelleta sellaiseen henkilötietojen käsittelyyn, jota yksityinen henkilö suorittaa henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa. Asia muuttuu siinä vaiheessa, kun mukaan tulee yrittäminen. Etenkin yksinyrittäjillä rajan vetäminen kotitalouden ja yritystoiminnan välille saattaa olla välillä vaikeaa. Siksi kannattaa heti aluksi miettiä tarkkaan, miten nämä kaksi asiaa erottaa selvästi toisistaan.

Tietosuoja

Tietosuoja-asetuksen takana on ajatus siitä, että kaikkia eurooppalaisia asiakkaita kohdellaan samalla tavalla ja heillä on samat oikeudet jokaisessa EU-maassa. Se on sinällään hienoa, koska yrittäjän ei tarvitse enää miettiä, mitä oikeuksia kenellekin kuuluu. Ihmisten oikeudet ovat kaikkialla samat ja jokainen yrittäjä voi luottaa tehneensä tarpeeksi, oli asiakas sitten mistä EU-maasta tahansa.

Tietosuojassa on kysymys siitä, että turvataan kaikkien luonnollisten henkilöiden (asiakkaiden, yhteistyökumppanien ja työntekijöiden) yksityisyydensuoja kaikessa toiminnassa. Asetuksella siis suojataan ensisijaisesti jokaisen ihmisen **kotirauhaa, kunniaa ja oikeutta yksityiselämään**. Mistään sen monimutkaisemmasta asiasta ei ole kyse.

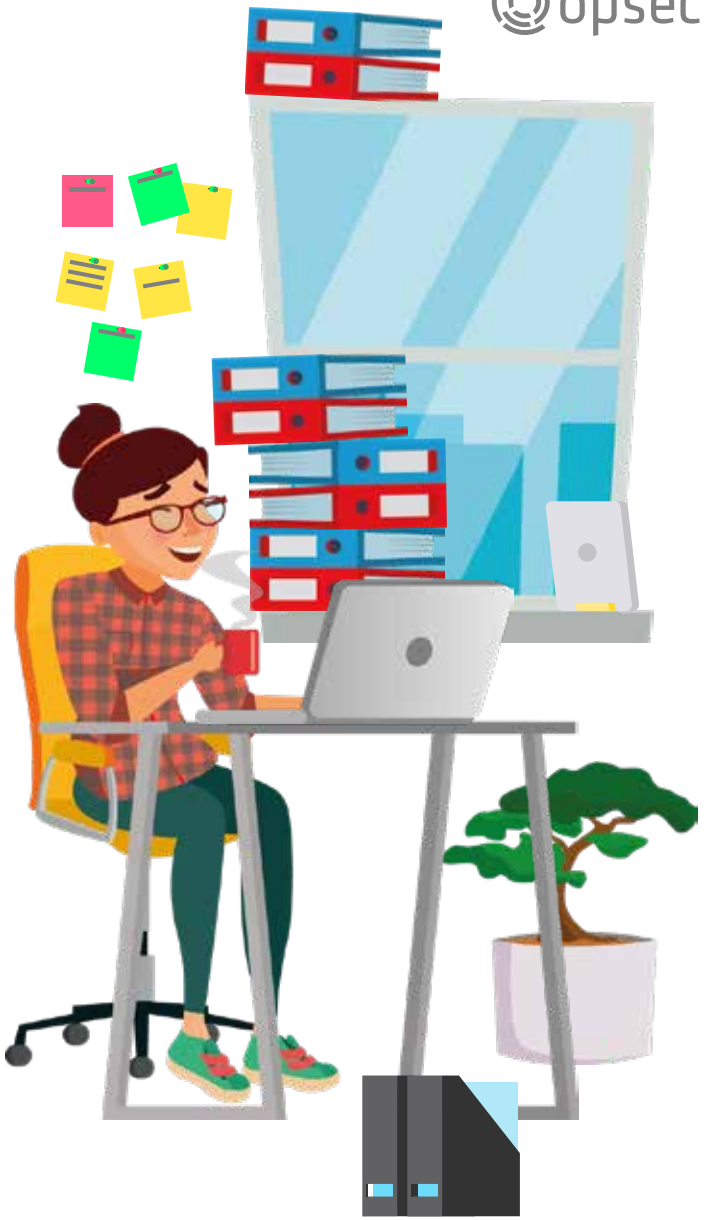
Jokainen yrittäjä Suomessa haluaa toimia siten, että asiakkaat ja alihankkijat luottavat häneen, joten nyt tuo luottamuksen ansaitsemisen minimiraja on myös kirjoitettu lakiin.

Aiheeseen tutustuminen

Jonkinlainen perustieto henkilötietojen käsittelystä ja tietosuojasta auttaa tulevassa tietosuojatyössä, joten hyvä lähtökohta on aloittaa kevyesti ja tutustua olemassa olevaan videokoulutusmateriaaliin.

Julkishallinnolle on olemassa erittäin hyvä peruskoulutus tietosuojasta, joten sitä kannattaa hyödyntää. Materiaali löytyy osoitteesta: arjentietosuoja.fi. Kaikkia sivuston videoita ei tarvitse katsoa, mutta suositeltavaa olisi katsoa ainakin noin puolen tunnin mittainen perustietoa sisältävä video: "*Arjen tietosuojaa - tietosuojaa meille kaikille*" [1].

Vaikka tietosuoja aiheuttaisi hiukan päänvaivaa, kannattaa muistaa, että myös itsellä on kaikki samat oikeudet asiakkaana ja kumppanina. Asiaan kannattaa siis tutustua jo siksi, että oppii tuntemaan omat oikeutensa.



Esimerkkiyritys: Hyvinvointikeidas Maija

Oppaassa käytetään esimerkkinä yritystä nimeltään Hyvinvointikeidas Maija. Esimerkkiyrityksen avulla oppaassa annetaan käytännön ohjeita ja vinkkejä tietosuojatyön eri vaiheisiin sekä dokumenttien täyttämiseen.

Oppaan mallilomakkeista ja -työkaluista löytyy esimerkkiyrityksen tietoja, mutta on huomioitava, että esimerkit ovat yleisluontoisia. Jokainen yritys käsittelee erilaista tietoa, joten esimerkkien tarkoitus ei ole toimia täydellisenä mallina, vaan niiden tarkoitus on helpottaa asian sisäistämistä ja johdattaa ajattelua oikeaan suuntaan. Pienelläkin yrityksellä saattaa olla paljon enemmän henkilötietoja ja tietosäilöjä kuin esimerkeissä on voitu nostaa esille.

Hyvinvointikeidas Maijan perustaja on Maija, joka on toiminut jo kymmenen vuotta yrittäjänä. Yrityksen alkuaikoina Maija työskenteli yksin tarjoamalla fysioterapiaan ja liikuntaneuvontaan liittyviä palveluja, mutta vuosien varrella hänen yrityksensä on vähitellen kasvanut.

Maijan yritys avasi muutama vuosi sitten oman kuntosalin, jonne Maija palkkasi Janitan ohjaajaksi. Janita osoittautui palkkauksen jälkeen hyväksi ohjaajaksi, joten tällä hetkellä hän tuottaa yrityksessä personal trainingiin (PT) ja liikuntaneuvontaan liittyviä palveluita kokopäiväisenä työntekijänä.

Janitan lisäksi Maija työllistää myös lapsiaan, Ronjaa ja Ronia. He toimivat apuna kuntosalin arjen pyörittämisessä osa-aikaisina työntekijöinä.

Fysioterapiapalveluiden kysyntä on myös kasvanut eikä Maija ole pystynyt enää yksin hoitamaan kaikkia asiakkaita. Tämän vuoksi Maija saa apua hierojapalveluita tuottavalta Juhalta. Juhalla on päätyö paikallisessa kylpylässä, mutta oman työn sesonkiluontoisuuden vuoksi hän ehtii auttamaan Maijaa. Juhalla on oma toiminimi, joten hän laskuttaa Hyvinvointikeidas Maijassa tekemistään työtunneista.

3. Henkilötietojen kartoittaminen

Kaiken lähtökohtana henkilötietojen ja rekisteröityjen oikeuksien suojaamisessa on kartoittaa, mitä henkilötietoa yrityksessä todella käsitellään, missä sitä on ja kenellä siihen on pääsy. Ajatuksena tämä on erittäin yksinkertainen, mutta käytännössä jo muutaman vuodenkin yrittäjänä toiminut on saattanut kerätä tietokoneen kiintolevyille, muutamaan pilvipalveluun ja ainakin yhteen sähköpostilaatikkoon tietoa muista ihmisistä.

Asiakkaista on usein yhteystietoja, laskutustietoja ja osoitteita. Omista työntekijöistä on palkanmaksuun, työterveyshuoltoon ja työajanseurantaan liittyviä tietoja. Asiakkaista ja työntekijöistä tallentuu usein myös tietoja kiinteistön kameravalvonnan tallentimelle tai markkinointia varten otettuihin valokuviin ja videoihin. Yritystoiminnan pyörittämisessä tarvitaan usein myös yhteistyökumppaneita, muita yrittäjiä, joten tarvitaan myös sopimuksia heidän palveluistaan ja henkilötietojen käsittelystä [(2.)].

Tässä vaiheessa ei tarvitse vielä miettiä, mitä tietoja saa kerätä tai miksi ja miten ne perustellaan. Tähän asiaan palataan myöhemmin tässä oppaassa. Tässä vaiheessa on tavoitteena kartoittaa ja tunnistaa kaikki henkilötieto, mitä yrityksellä on ja missä se sijaitsee. Asioita ei tarvitse vielä miettiä liikaa eteenpäin, vaan kannattaa keskittyä nykytilan kartoittamiseen.

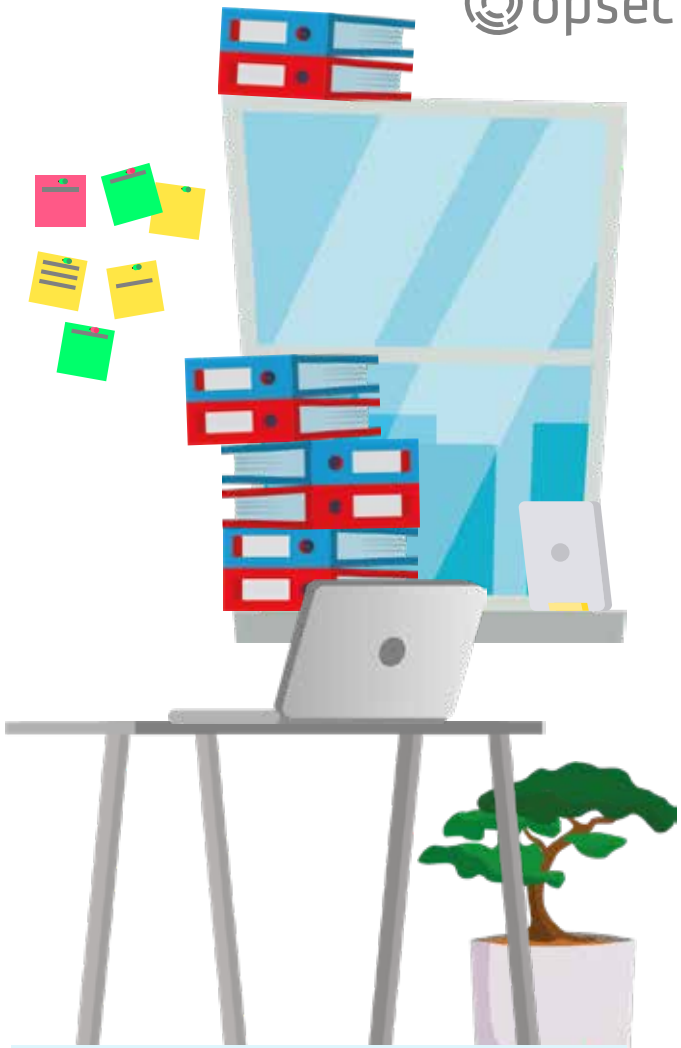
Henkilötietojen kartoittaminen aloitetaan kirjaamalla ja keräämällä henkilötietoja ja niiden sijainteja lomakkeelle, miettimättä vielä sen kummemmin, mitä tiedoille jatkossa tehdään. **Tätä vaihetta varten voi ottaa esille oppaan liitteenä olevan lomakkeen 1**. Jatkotyön helpottamiseksi kannattaa tiedot jaotella kokonaisuuksiin esimerkiksi sen mukaan, kenestä tiedot ovat (esim. asiakkaat, työntekijät ja yhteistyökumppanit). Se helpottaa myös tietojen keräämisvaihetta, kun voi keskittyä yhteen ryhmään kerrallaan.

Lomakkeen voi tulostaa ja täyttää käsin, jos se tuntuu luontevalta tavalta tai lomakkeesta voi tehdä oman tiedoston tietokoneella. Tietosuojalainsäädännön kannalta ei ole väliä, miten tiedonkeruu tehdään, kunhan asiat ovat jossain dokumentoituna ja tallessa.

Seuraavilla sivuilla on kerrottu, miten Maija aloitti työskentelyn. Tämän osion lopusta löytyy myös Maijan täyttämä mallilomake hänen keräämistä henkilötiedoista.

Henkilötietoa *on kaikki sellainen tieto, josta yksittäinen henkilö on tunnistettavissa. Nimi, sähköpostiosoite, auton rekisterinumero, valokuva, asiakasnumero, työntekijän veronumero tai, mikä tahansa tieto, joka voidaan jotenkin yhdistää yksittäiseen henkilöön.*

Myös kaikki tieto, joka on liitettävissä johonkin henkilöön suoraan tai epäsuorasti, lasketaan henkilötiedoksi. Jos esimerkiksi laskulla on asiakasnumero, on laskulla oleva tieto liitettävissä henkilöön.



Henkilötietojen käsittely *on henkilötietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä ja muokkaamista. Henkilötietojen käsittelyä ovat myös haut ja kyselyt sekä henkilötietojen käyttäminen, luovuttaminen (siirtämällä, levittämällä tai asettamalla ne muutoin saataville), yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja tuhoaminen.*

Henkilötiedot Hyvinvointikeidas Maijalla

Maijan henkilötietojen kartoituksen alku tuntui toivottomalta. Henkilötietoa oli joka paikassa. Ei ollut sellaista kansiota, pilvipalvelua, tietojärjestelmää tai sähköpostilaatikkoa, jossa ei olisi ollut jonkun tietoja. Maijalla oli yrityksessä käytössä pilvipalveluna ostettu verkkolevyasema, josta oli helppo jakaa tietoa myös Juhalle ja Janitalle. Mutta se tuntui olevan täynnä kaikkea mahdollista ja hirveässä epäjärjestyksessä.

Maija päätti aloittaa henkilötietojen kartoituksen siivouspäivällä. Ensiksi hän siirsi kaikki tiedot talteen verkkoasemalle. Sen jälkeen hän poisti kaikki sekalaisia tietoja sisältävät Dropboxit ja lähinnä valokuvia sisältävät Flickr -tilit, joita oli perusteltu aina tarpeen mukaan sinne tänne. Hän järjesteli myös verkkolevyaseman uudestaan. Maijan yritys on käsittelemiensä henkilötietojen rekisterinpitäjä ja rekisterinpitäjän on aina tiedettävä, missä tietoa on ja kuka siihen pääsee käsiksi, joten hänen tuli järjestää tiedot uudelleen.

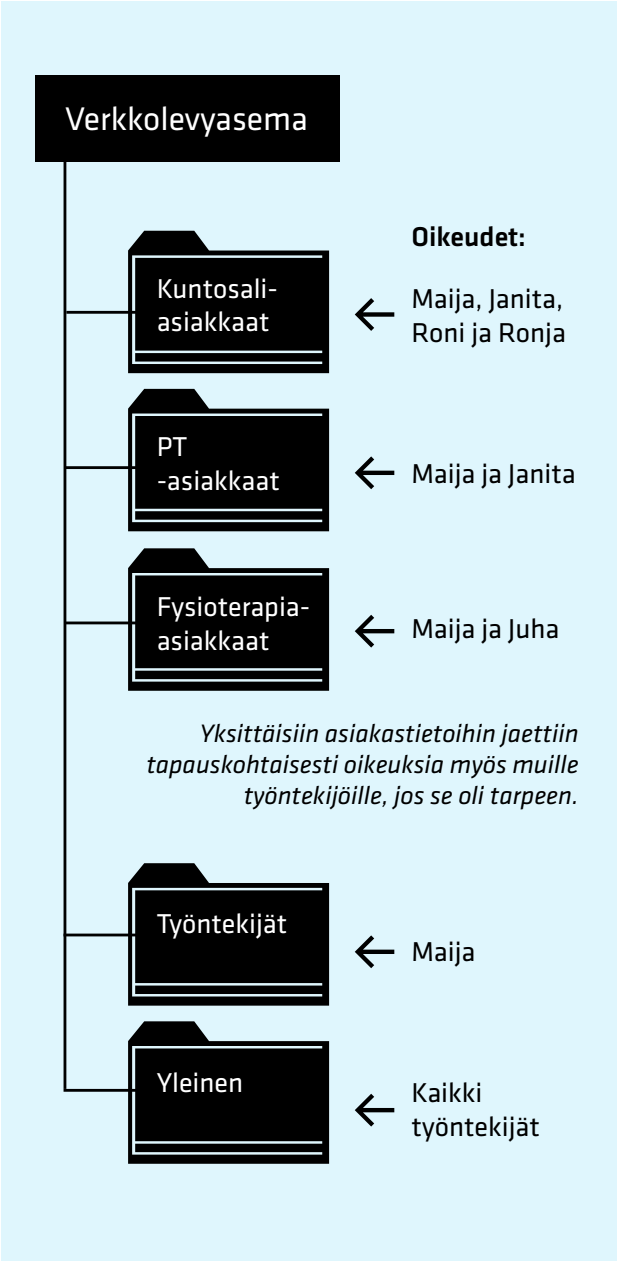
Maija jakoi asiakastietonsa kolmeen pääryhmään: kuntosali, PT ja fysioterapia. Kuntosaliasiakkaiden tietoihin piti päästä kaikkien salilla työskentelevien ja PT-asiakkaiden tietoihin Maijan ja Janitan. Tapauskohtaisesti asiakkaiden tietoja jaettiin myös Juhalle, mutta lähtökohtaisesti kaikkea asiakastietoa ei kuitenkaan tarvinnut hänelle jakaa. Fysioterapia-asiakkaiden tietoihin annettiin pääsy Maijalle ja Juhalle. Fysioterapia-asiakkaiden tietoja ei voinut jakaa kaikille kuntosalilla työskenteleville, sillä fysioterapian tietoihin sisältyi usein asiakkaan arkaluonteista terveystietoa. Esimerkiksi lääkärien lähetteet, Kelan lausunnot ja vastaavat olivat sellaista tietoa, jota ei voinut jakaa kaikille työntekijöille.

Työntekijöiden tiedot (työsopimukset, sairaslomatodistukset ja vastaavat tiedot) Maija keräsi yhteen kansioon. Ja, koska hän hoiti henkilöstöhallintoa yksin, hän ei antanut muille käyttöoikeuksia kansioon.

Sitten Maija tarvitsi vielä Yleinen -kansion, jossa hän saattoi jakaa kaikille työntekijöille tarpeellisia tiedotteita ja käytäntöjä. Verkkoaseman siivouksen jälkeen Hyvinvointikeidas Maijan pääkansiorakenne näytti viereisen kuvan kaltaiselta.

Tulevan tietosuojaprojektin vuoksi Maija myös loi Yleinen -kansioon Tietosuoja nimisen kansion, johon hän päätti koota kaiken tietosuojaprojektiin liittyvän materiaalin. Tietosuoja -kansioon hän teki julkisen osion, johon hän päätti kerätä kaikille työntekijöille tarkoitetut dokumentit ja ohjeet. Toisen osion hän teki itselleen projektin työvaiheita ja tallessa pidettäviä dokumentteja varten. Projektin aikana oli tulossa paljon erilaista dokumentaatiota, joten oli järkevää kerätä ne kootusti yhteen paikkaan.

Siivouksen aikana Maija mietti käyttöoikeuksia myös muualla liiketoiminnassaan; kuka työntekijöistä tarvitsi pääsyn yrityksen yleiseen sähköpostilaatikkoon ja kenen tarvitsi päästä kirjanpito-ohjelmaan - ja ketkä eivät tarvinneet pääsyä noihin järjestelmiin.



Maija teki siivousurakan myös paperiselle aineistolle. Mappien uudelleen järjestely ja niiden sijoittelu siten, että ne olivat vain sellaisten henkilöiden saatavilla, jotka tarvitsivat niitä, selkiytti myös toimintatapoja. Paljon tietoa päätyi myös roskikseen. Arkaluonteiset paperit Maija silppusi toimiston silppurilla. Maija olisi voinut käyttää myös tiedon turvalliseen tuhoamiseen tarkoitettua tietosuoja-astiaa, mutta tulostettua materiaalia oli kertynyt Maijalla niin vähän, ettei astiaa ollut tarvinut hankkia.

Urakan jälkeen Maija täytti lomakkeen 1. Maija päätti lomaketta täyttäessään ja jatkotyötä helpottaakseen jakaa henkilötiedot sellaisiin ryhmiin, joille hän joutuisi laatimaan myös selosteita henkilötietojen käytöstä (tähän asiaan palataan oppaan 8. osassa). Tällainen tiedon jakaminen erilaisten henkilöryhmien mukaan helpottaisi myös Maijan seuraavaa työvaihetta, sillä usein tietojen käyttötarkoitukset vaihtelevat eri ryhmien välillä.

Tällainen verkkolevyjen ja paperisten tietojen siivousurakka voi tuntua kovalta työltä, mutta loppujen lopuksi se selkeyttää ja helpottaa koko yrityksen toimintaa. Turhan tiedon poistaminen täyttää myös tietosuojalainsäädännön henkilötiedon minimoinnin velvoitetta ja säilytyksen rajoittamisen velvoiteita [(3.)]. Oppaan seuraavasta osassa on käsitelty tarkemmin sitä, miksi turhaa tietoa ei tule säilyttää, mutta nyt tässä vaiheessa keskititytään kartoittamaan kaikki henkilötiedot, joita yrityksessä käsitellään.

Tietojen minimointi *tarkoittaa, että käsitellään henkilötietoja vain siinä laajuudessa kuin se on tarpeen, eikä kerätä turhia tietoja. Säilytyksen rajoittaminen viittaa siihen, että huolehditaan henkilötiedon asianmukaisesta poistosta, kun sille ei enää ole tarvetta.*

Erityisen arkaluonteisia henkilötietoja*, ns. erityistietoryhmiä, ovat tietosuojalainsäädännön näkökulmasta terveystiedot, ihmisten uskontoa, vakaumusta tai poliittista mielipidettä koskevat tiedot, seksuaalinen suuntautuminen sekä rotuun ja etniseen alkuperään liittyvät tiedot.*

Lomake 1 (Hyvinvointikeidas Maija)

Ketä tieto koskee?	Missä tietoa on?	Mitä tieto on (yleiskuvaus)?
Asiakkaat	- Verkkolevyasema (word- ja pdf-tiedostoja kansioissa) - Vastaanoton tietokone - Sähköposti (info@hyvinvointikeidasmaija.fi) - Kirjanpito-ohjelma (laskutus) - Paperiarkisto	- Kuntosaliasiakkaiden sopimukset (Sopimus-kansio) - Fysioterapia-asiakkaiden ohjelmat (Fysioterapia-kansio) - Personal training -ohjelmat (PT-kansio) - Postituslistat excelissä - Osallistujalistoja ryhmäjumppatunneilta - Kirjeenvaihto ja asiakkaiden lähettämät liitteet, yms. - Asiakkaiden laskut ja maksuhistoria - Alkuperäiset kuntosaliasiakkaiden sopimukset
Työntekijät	- Verkkolevyasema - Kirjanpito-ohjelma (palkanlaskenta) - Paperiarkisto - Internet-sivut	-Työsopimukset -Työhakemukset - Palkanmaksutiedot - Palkkahistoria - Palkkakuitit - Sairaslomatodistukset - Työntekijöiden yhteystiedot ja valokuvat
Sopimuskumppanit	- Verkkolevyasema - Kirjanpito-ohjelma (ostolaskut)	- Sopimukset - Laskut ja laskuhistoria

4. Henkilötietojen käsittelyn tarkoitusten ja lainmukaisuuden selvittäminen

Tässä osassa käsitellään sitä, miksi Maija päätyi edellisessä vaiheessa vähentämään ja poistamaan vanhaa tietoa. Monet ihmiset ovat tavaran ja omaisuuden suhteen keräilijöitä, joiden on vaikea luopua juuri mistään. Siksi myös jokainen yritys on keräilijä, mitä tulee yrityksen omistamaan tietoon. Mitään ei heitetä pois ja tietoa vaan kertyy ja kertyy vuosien saatossa. Ajatellaan, että kaikki pitää säästää, koska ikinä ei tiedä, milloin tietoa tarvitsee. Tosiasia on kuitenkin se, että todella harvoin pari vuotta vanhaa dokumenttia kukaan enää tarvitsee. Usein vanhoja dokumentteja availlaan vain siksi, että niitä luullaan uusimmiksi versioiksi. Näin tietojen etsijä tekee usein myös turhaa työtä, ennen kuin löytää etsimänsä.

Tietosuojalainsäädäntö velvoittaa yrityksiä miettimään, mitä tietoa on todella tarve kerätä ja mitä ei, mutta asiaa kannattaa muutenkin pohtia. Usein turha tieto, kuten monet eri versiot samasta dokumentista ja hyllymetrit turhaa paperia vain vaikeuttavat ja hidastavat liiketoimintaa. Siivousurakka kannattaa siis tehdä sekä tietosuojan että liiketoiminnan tehokkuuden vuoksi.

Tietoa ei kuitenkaan kannata suinpäin innostua poistamaan, jos ei ole tässä vaiheessa vielä varma tarvitseeko kyseistä tietoa jatkossa ja saako kyseistä tietoa säilyttää vai ei. Poistettava tieto kannattaa kirjata ylös, jotta siihen voi palata sen jälkeen, kun on käynyt läpi tämän oppaan eri vaiheet.

Henkilötietojen käsittelyn tarkoitus

Tietosuojalainsäädännön näkökulmasta pitää täyttyä pari asiaa, jotta henkilötietoa (tai tietoa, joka sisältää henkilötietoa) voidaan ylipäätään säilyttää ja käsitellä.

Kaikella henkilötietojen käsittelyllä tulee olla aina jokin tarkoitus. Tarkoituksia on joskus useampiakin, mutta ne on tunnistettava ja niistä on kerrottava niille henkilöille, joiden tietoja käsitellään. Sen lisäksi tietoa ei saa käsitellä mihinkään muihin tarkoituksiin kuin henkilöille ilmoitettuihin tarkoituksiin. Tätä tarkoittaa lainsäädännössä mainittu käyttötarkoitussidonnaisuus.

Usein asiakkaiden tietoja käsitellään hyvin eri tarkoituksiin kuin esimerkiksi työntekijöiden tietoja. Tämän vuoksi esimerkkiyrityksen Maijakin käytti rekisteröityjen ryhmiä jaotteluperusteena täyttäessään lomaketta 1.

Henkilötietojen käsittelyn lainmukaisuusperuste

Kaikkein tärkeintä siis on, että henkilötiedon keruulle, säilyttämiselle ja käsittelylle on lainmukainen käsittelyperuste [(4.)]. Henkilötiedon käsittely on lainmukaista vain seuraavissa tapauksissa:

1. **Henkilö on sopimusosapuolena yritykseen, joka käsittelee hänen henkilötietoaan**

Olemassa olevat sopimusasiakkaat, työsuhteessa olevat työntekijät tai sopimussuhteessa olevat palveluiden toimittajat. Kohtuullisuusvaatimuksen vuoksi tämän ryhmän tietoja voi käsitellä vain siinä laajuudessa kuin sopimus edellyttää.

2. **Henkilötietojen käsittely on tarpeen yritystä koskevan lakisääteisen velvoitteen noudattamiseksi**

Tämä laajentaa usein kohtaa 1. Esimerkiksi asiakkaan laskuja koskevia tietoja on säilytettävä kirjanpitolain mukaan 10 vuotta tilikauden päättymisestä. Työntekijöille on kyettävä toimittamaan työtodistus 10 vuotta työsuhteen päättymisestä, mikä tarkoittaa joko työtodistuksen tai sen antamiseen tarvittavien tietojen säilyttämistä 10 vuoden ajan.

Työlainsäädäntö, vuosilomalaki ja vaikkapa laki työterveyshuollon järjestämisestä tuovat myös oman lisänsä työntekijöiden tietojen käsittelyyn.

Henkilötietoja saa säilyttää vain siinä laajuudessa kuin laki edellyttää, joten vaikka työtodistus pitää kyetä toimittamaan vuosia jälkikäteen, ei yritys voi mitenkään perustella, miksi se säilyttäisi vuosikausia vaikkapa työntekijän kehityskeskustelujen muistiinpanoja.

3. Käsittelyyn on henkilön suostumus

Henkilötietoja saa käyttää vain niihin käyttötarkoituksiin, joihin suostumus on saatu ja vain niin kauan kuin suostumus on voimassa. Kenellä tahansa on oikeus peruuttaa suostumuksensa koska tahansa.

Koskee esimerkiksi henkilöitä, joille on saatu lupa lähettää mainoskirjeitä (tai muuta markkinointiviestintää).

Suostumusta ei suositella käytettäväksi työsuhteissa, sillä suostumuksen pitää olla vapaaehtoisesti annettu. Johtuen työnantajan valta-asemasta työntekijöihin nähden, suostumusta ei useinkaan voida pitää vapaaehtoisesti annettuna.

4. Rekisterinpitäjän oikeutettu etu

Tähän kategoriaan menee tavanomaisimmin sellainen henkilötiedon käsittely, jolle ei ole suoraa oikeutta lainsäädännössä ja, jolle on hankala kerätä esimerkiksi suostumusta, mutta tieto on silti tärkeää yritykselle. Esimerkiksi toimitilojen kameravalvonta, jossa oikeutettu etu on yrityksen omaisuuden suojaaminen. Myös suoramarkkinointi yritysten normaalissa liiketoiminnassa usein lasketaan tämän alle. Oikeutettu etu on silloin elinkeinon harjoittaminen, jota pyritään edistämään markkinoinnilla.

Oikeutettu etu on aina nimettävä. Se ei voi olla mikään keksitty tarve, vaan se on oltava todellinen. Lisäksi henkilöille, joiden tietoja käsitellään, ei saa koitua siitä vahinkoa.

Yrityksen on tehtävä kirjallinen tasapainotesti osoittaakseen, että rekisterinpitäjän oikeutetut edut ovat tosiaan suuremmat kuin rekisteröityjen oikeudet ja vapaudet.

Henkilöillä on aina oikeus vastustaa henkilötietojensa käsittelyä, kun se perustuu oikeutettuun etuun. Jos yritys ei voi osoittaa, että sen omat edut menisivät luonnollisten henkilöiden oikeuksien ja vapauksien edelle, on käsittely lopetettava.

Oikeutetusta edusta suoramarkkinoinnissa ja suoramarkkinoinnin tasapainotestistä kerrotaan lisää oppaan 11. osassa.

Henkilötietojen käsittelijän rooli

Henkilötietojen käsittelyn roolille kannattaa antaa pari ajatusta. Lainsäädännössä puhutaan rekisterinpitäjästä ja henkilötietojen käsittelijästä [5.]. Rekisterinpitäjä on sellainen yritys, jonka vuoksi tietoja käsitellään ja joka voi itse yksipuolisesti määritellä, mihin tarkoituksiin ja miten tietoja käsitellään. Suurin osa suomalaisista yrityksistä on lähes sataprosenttisesti omistamiensa henkilötietojen rekisterinpitäjä.

On myös sellaisia toimialoja, joilla asia voi olla päinvastoin. Tällaisia toimialoja ovat usein esimerkiksi tilitoimistot ja IT-palveluita tarjoavat yritykset. Nämä yritykset ovat käsittelijöitä, sillä ne käsittelevät henkilötietoja vain niihin tarkoituksiin ja vain siinä laajuudessa kuin tilaaja (rekisterinpitäjä) on määritellyt. Esimerkiksi pilvipalveluiden tarjoaja usein tarjoaa tilaajalle vain ohjelmiston, jonne yritys voi viedä vaikka asiakasrekisterinsä tai markkinointinsa sähköpostilistat. Palveluntarjoaja ei käytä tilaajayrityksen (rekisterinpitäjän) tietoja mihinkään omiin tarkoituksiinsa. Esimerkiksi tilitoimisto maksaa palkkoja vain niille ihmisille ja siten kuin tilaaja (rekisterinpitäjä) asian määrittelee.

Käsittelijä voi olla myös silloin, kun yrityksellä on pääsy toisen yrityksen henkilötietoihin, vaikka tietoja ei varsinaisesti käsitelläkään. Esimerkiksi IT-tuella on usein hallussaan asiakkaidensa käyttäjätunnukset ja salasanat järjestelmiin ja he pääsevät niihin myös käsiksi suorittamiensa tukipalveluiden ohessa. Pelkästään pääsy toisen yrityksen henkilötietoihin vaikuttaa lakisääteisiin velvoitteisiin. Esimerkiksi siihen, että tällaisesta suhteesta henkilötietojen käsittelystä on aina oltava sopimus. Sopimuksista kerrotaan lisää 6. osassa.

Seuraava toimenpide kohti lainmukaista henkilötietojen käsittelyä tehdään lomakkeen 2 avulla. Tässä vaiheessa täytetään yksi lomake jokaisesta sellaisesta tietojoukosta, joka muodostaa jollain tavalla käsittelyn tarkoitusten ja lainmukaisuuden osalta tietynlaisen loogisen kokonaisuuden. Lomakkeen 1 ensimmäinen sarake kertoo, montako lomaketta tässä vaiheessa täytetään. Jos lomakkeen ensimmäisestä sarakkeesta löytyy kaksi ryhmää, täytetään tässä vaiheessa kaksi lomaketta. Jos ensimmäisessä lomakkeessa on kolme ryhmää, täytetään tässä vaiheessa kolme lomaketta. Jne.

Laissa ei sanota, miten nämä kokonaisuudet pitää koota, vaan tärkeää on se, että ne ovat yrittäjälle itselleen loogisia ja tarkoituksenmukaisia. Hyvä neuvo on pitää ryhmien määrä mahdollisimman vähäisenä. Jokaisen pikkupoikkeuksen takia ei kannata perustaa uutta ryhmää henkilötietoja.

Yrittäjän on myös hyvä muistaa, että jos yrityksessä on enemmän työntekijöitä, kannattaa tietosuojatyöhön osallistaa muutkin. Etenkin, jos tietoa on niin paljon, ettei yrittäjä tee enää yksin kaikkea yrityksen tietojen käsittelyyn liittyvää työtä.

Hyvinvointikeidas Maijan henkilötietojoukot ja henkilötietovirrat

Maija päätti tehdä kartoitustyön itse, sillä hän oli ainoa, joka yrityksessä tunsi kaikki tiedot ja niiden käsittelytavat ja säilytyspaikat.

Maija löysi edellisessä vaiheessa kolme päätietojoukkoa (ryhmää) lomakkeelle 1; asiakkaat, työntekijät ja sopimuskumppanit. Seuraavaksi hän etsi näiden tietojoukkojen osalta tärkeät tunnistettavat tiedot. Maija aloitti asiakkaista, sillä hän oli eniten huolissaan siitä, että saisi asiakkaita varten tietosuojaselosteet ja asiat kuntoon siten, että heidän kysymyksiinsä osattaisiin vastata. Lisäksi Maijan yrityksessä oli hyvin avoin ilmapiiri ja monia muita työhön liittyviä asioita jaettiin kaikkien työhön osallistuvien kesken. Työsuhteita oli myös vähän, joten Maija siirsi näiden tietojen osalta jatkotyöstämisen rauhallisempaan aikaan.

Maijan asiakastiedoista tekemä tarkempi kartoitus näyttää seuraavan sivun lomakkeen 2 mukaiselta. Huomaa, että siellä oleviin kohtiin *Käsittelijöistä* ja *Henkilötietojen siirroista Eta-alueen ulkopuolelle* palataan oppaan 6. osassa sekä *sähköpostimarkkinointiin* oppaan 11. osassa.

Tässä vaiheessa Maijalla oli hyvä käsitys siitä, mitä henkilöihin liittyvää tietoa hänellä oli asiakkaistaan. Maijalle oli kuitenkin vielä hiukan epäselvää, miten tieto liikkui ja missä sitä kulloinkin oli ja kenen vastuulla. Sen vuoksi Maija päätti vielä tarkastella asiakkaidensa tietojen liikkeitä tietovirtojen kuvaamisen kautta.

Tietovirtojen tarkastelu auttoi Maijaa hahmottamaan sitä, mistä yritykseen tuli henkilötietoa, mihin sitä meni ja mitä sille tapahtui, kun sitä ei enää tarvittu.

Tätä varten Maija täytti lomakkeen 3, jossa oli pystysarakkeilla tiedon elinkaaren kolme tärkeintä vaihetta; tietojen keruuvaihe, säilytysvaihe ja poistamisvaihe. Vaakariveillä Maija kuvasi sitä, kuka osallistui missäkin vaiheessa asiakastiedon käsittelyyn.

Maijan täyttämät lomakkeet 2 ja 3 löydät seuraavilta sivuilta.

Lomake 2 (Hyvinvointikeidas Maija)

Henkilötietojoukko ja yrityksen rooli (rekisterinpitäjä vai käsittelijä)	Hyvinvointikeidas Maijan asiakkaat, rekisterinpitäjä Hyvinvointikeidas Maija (Y:1234567-0), Sijainnit: Verkkolevyasema, vastaanoton tietokone, Maijan tietokone, sähköposti (info@hyvinvointikeidasmaija.fi), kirjanpito-ohjelma (laskutus-moduli), paperiarkistot (mapit)
Mitä henkilötietoa tietojoukko sisältää?	Asiakasnumero, nimi, osoite, puhelinnumerot, katuosoite (laskutusosoite, jos eri), sähköposti ja suoramarkkinointikiellot tai muut rajoitukset. - Kuntosali- ja PT-asiakkaista tallennetaan lisäksi sopimustiedot (jäsenyystaso, voimassaoloaika, alkupvm, keskeytykset ja sopimuksen sen hetkinen tila ja mahdollinen syy sekä PT-ohjelmat ja niiden seuranta. - Fysioterapia-asiakkaista on asiakaskohtaisissa kansioissa lisäksi lääkärien lähetteet, Kela-korvauksiin liittyvät asiakirjat, ohjelmat ja niiden seurantatieto.
Käsittelijät *(6. osassa tästä aiheesta lisää)*	Tilitoimisto (sopimuskumppani), palvelinylläpitäjä (tilitoimiston alikäsittelijä ja sopimuskumppani), IT-tuki, Mailchimp (sähköpostimarkkinointi/uutiskirjetyökalu)
Henkilötietojen siirrot Eta-alueen ulkopuolelle *(6. osassa tästä aiheesta lisää)*	Henkilötietoja ei siirretä ETA-alueen ulkopuolelle muuten kuin asiakkaiden uutiskirjelistojen osalta. Kyseessä on ohjelma nimeltä Mailchimp, jonka postituslistat sijaitsevat yhdysvaltalaisella palvelimella. Siirron perusteena on EU-US Privacy Shield järjestely ja Yhdysvaltain liittovaltion kauppaministeriön voimassaoleva auditointi yhtiölle (The Rocket Science Group LLC d/b/a MailChimp).
Käsittelyn tarkoitus	Kuntosali, PT- ja fysioterapia-asiakkaille kyseisten palveluiden tarjoaminen ja asiakkaiden laskutus.
Käsittelyn lakiperuste	Sopimussuhde yritykseen. Suoramarkkinointiasiakkailta on kerätty suostumus tiedotteiden ja uutiskirjeiden lähettämiseen.
Erityistietoryhmät ja erityiset rekisteröityjen ryhmät	Fysioterapia -asiakkaiden terveydentilaan ja sairauden hoitoon tai kuntoutukseen liittyvät asiat. Paperiaineistoa sekä sähköinen aineisto verkkolevyllä asiakkaan omassa kansiossa.

Lomake 3 (Hyvinvointikeidas Maija)

	Henkilötietojen kerääminen	Henkilötietojen säilytys ja käsittely	Henkilötietojen poisto ja ulos siirrot
Asiakas	Asiakas tulee ja haluaa sopimuksen ja luovuttaa tietonsa. Asiakas luovuttaa tietonsa myyntitapahtumassa myöhempää yhteydenottoa tai markkinointia varten	Asiakas voi haluta korjata tietojaan tai toimittaa lisätietoja esimerkiksi fysioterapian toteuttamiseksi tai kuntosalijäsenyyden väliaikaiseksi keskeyttämiseksi. Myös suoramarkkinointikielto tulee asiakkaalta.	Asiakas voi pyytää poistamaan tarpeettomia tietoja tai yhteystietonsa postituslistoilta
Yritys	Kerää asiakkaalta laskutustiedot ja tuottaa palveluiden käytön seurantaan liittyvää tietoa (kuntosalijäsenyys, PT-ohjelmat, fysioterapiaohjelmat ja niiden seuranta)	Verkkolevyasema, vastaanoton tietokone, Maijan tietokone, sähköposti (info@hyvinvointikeidasmaija.fi), kirjanpito-ohjelma (laskutus-moduli), paperiarkistot (mapit)	Asiakkaiden kansiot ja paperiaineisto poistetaan asiakkuuden päättyessä. Kirjanpitoaineisto säilytetään 6 vuotta ja siirretään sitten tilitoimistolle.
Tilitoimisto	Tilitoimistolle kertyy asiakkaan maksuhistoria ja siihen liittyvät tiedot.	Säilyttää laskutukseen liittyvää asiakas tietoa tietojärjestelmässään, jota Maija vuokraa.	Tilitoimisto hävittää tositteet 10 vuoden kuluttua. Tilitoimistolla on arkistontuhoussopimus ulkoisen toimittajan kanssa paperiaineiston osalta.
IT-tuki	Ei kerää tai tuota asiakkaisiin liittyvää tietoa	IT-tuki pääsee näkemään asiakastietoja vikojen ja ongelmien selvityksen yhteydessä, mutta ei saa muokata niitä.	IT-tuki tuhoaa sopimuksen mukaan Maijan käytöstä poistuvilta tietokoneilta kaikki tiedot.

5. Riskienhallinta

Tässä vaiheessa on jo aika hyvin selvillä, mitä ja millaista tietoa yrityksessä kerätään, missä sitä käsitellään ja kuka siihen missäkin roolissa osallistuu. Seuraavaksi siirrytään erääseen tietosuojalainsäädännön tärkeimmistä kokonaisuuksista, riskienhallintaan.

Pieni ajatusleikki pohdittavaksi: *Mitä tekisit, jos poliisi pysäyttäisi sinut tien viereen ja vaatisi sinua todistamaan, että ajoit töistä kotiin tieliikennelain mukaan?* Jos et pystyisi todistamaan tätä vaadittua asiaa, siitä saattaisi tulla sinulle seurauksia.

Näin on käytännössä tietosuojalainsäädännön kanssa, johon on sisäänrakennettu rekisterinpitäjän osoitusvelvollisuus. Jokaisen rekisterinpitäjän on kyettävä osoittamaan, että asetusvelvoitteita on noudatettu. Velvoite lähtee tietosuojaan liittyvien riskien tunnistamisesta ja arvioinnista, ja jatkuu aina kontrollikeinojen toteuttamiseen saakka.

Tietosuojavaltuutettu Reijo Aarnio totesi Kyberturvallisuuspäivillä 11.10.2017 puheenvuorossaan, että kun tietosuojan kanssa menee jotain pieleen, tulee ensimmäinen kysymys olemaan yritykselle: "*Miten arvioitte tietosuojaanne kohdistuvat riskit? Ja miten tämä tapahtuma oli ennalta huomioitu?*"

Organisaation on siis kyettävä perustelemaan, miten toteutunut riski on tunnistettu, miten siihen on varauduttu ja, miksi se siitä huolimatta pääsi toteutumaan. Ellei tätä työtä ole tehty, on kyse mahdollisesti jopa tuottamuksellisesti aiheutetusta vahingosta.

Vaikka tietosuoja vaatii hieman resursseja organisaatiolta, on tietosuojalainsäädännössä hyvätkin puolensa. Se nimittäin pakottaa organisaatiot toimimaan laadukkaasti, hyvin ja tehokkaasti. Sitä moni toki tavoittelee, mutta suurin osa haluaisi sen ilmaiseksi. Jos siis, haluat hyvin toimivan organisaation, sen laadunhallintaan on kiinnitettävä huomiota. Riskit on tunnistettava, niihin on varauduttava ja varautumista on suunniteltava sekä toteutukset tehtävä. Ja, kun tämä tehdään hyvin ja dokumentoidusti, tulee samalla noudattaneeksi lakia [6.]. Tie menestykseen vaatii kuitenkin jonkin verran työtä.

Riskien tunnistaminen ja käsittely

Riskienhallintaan on monia eri metodeja. Jos asia on täysin uutta, voi asiassa edetä tämän oppaan avulla. Jatkokehitystä ajatellen kannattaa riskienhallintaan kuitenkin perehtyä hiukan lisää.

Riskienhallinnan etenemistapa on yleensä seuraava (kursiivilla tekstillä on myös kerrottu Hyvinvointikeidas Maijan esimerkkitilanne riskienhallinnasta):

1. Riskien tunnistaminen

Mahdolliset riskit omasta toiminnasta on kyettävä tunnistamaan, koska tunnistamattomia riskejä ei voi hallita.

Lähtökohtana riskienhallintaan voi esimerkiksi olla tilannekohtainen arvio. Maijan Hyvinvointikeitaalla tyypillinen asiakaspalvelutilanne tiskillä pilkottiin osiin vaihe vaiheelta ja arvioitiin, että missä sen vaiheessa voisi tapahtua jotain odottamatonta.

2. Riskien analysointi

Tämä sisältää riskin tarkemman kuvaamisen ja erityisesti syiden, seurausten ja todennäköisyystekijöiden pohdinnan.

Hyvinvointikeidas Maijan asiakaspalvelutilanteessa (1. kohdassa mainittu) oli havaittu, että jonotettaessa vastaanottotiskille saattaa asioivan asiakkaan takana seisova, toinen asiakas, kuulla edellä asioivan henkilötietoja. Joten seuraavaksi riskiä arvioitiin tarkemmin: Miten usein asiakkaat joutuvat jonottamaan (ts. kuinka todennäköinen tilanne on)? Mitä ja miten arkaluonteista tietoa tilanteessa tyypillisesti vaihdetaan? Ovatko asiakkaat sellaisessa suhteessa toisiinsa, että he voisivat käyttää kuulemaansa tietoa väärin? Jne.

3. Riskien arviointi

Riskien merkityksen arvioinnin tärkein tavoite on saada kaikki tunnistetut ja analysoidut riskit tärkeysjärjestykseen. Millään yrityksellä ei ole resursseja poistaa kaikkia toimintansa riskejä, joten on tärkeää tietää, mihin pitää keskittyä ja millaisia riskejä toiminnassa voidaan sietää.

Edellisen esimerkin riskitilanne oli Maijalla epätodennäköinen. Fysioterapia- ja PT-asiakkaat, joilla oli arkaluonteisinta tietoa, saapuivat varatulle ajalle yksi kerrallaan ja tapaaminen aloitettiin aina Janitan tai Juhan kanssa suljetussa toimistotilassa. Kuntosali -asiakkaidenkaan ei tarvinnut asioida tiskillä, sillä he

pääsivät kuntosalille omalla kulkukortillaan. Heidän osalta arkaluonteisin tieto oli usein säästä keskustelua ja kuulumisten vaihtoa.

4. Riskien käsittely

Riskin käsittelyvaiheessa päätetään, mitä riskille tehdään. Riski voidaan käytännössä:

- pitää eli päätetään, ettei riskille tehdä mitään
- poistaa eli muutetaan olosuhteita siten, ettei riski pääse toteutumaan
- pienentää eli esimerkiksi muuttaa riskin todennäköisyyttä tai seurauksia pienemmäksi
- siirtää eli esimerkiksi vakuuttaa tai ulkoistaa toimintoja, jolloin riski ja sen seuraukset siirretään itseltä pois

Maija arvioi, että vaikka asiakastietojen joutuminen ulkopuoliselle olisi asiakaspalvelutilanteessa epätodennäköinen, se olisi silti hyvin ikävä henkilölle. Etenkin, jos asiakaspalvelutilanteessa käsiteltäisiin sairauksiin liittyviä tietoja. Niinpä Maija lisäsi verkkolevyaseman Yleinen -kansioon asiakaspalveluohjeen ja koulutti sen seuraavassa viikkopalaverissa kaikille työntekijöilleen. Ohjeessa kerrottiin, missä ja miten asiakkaan luottamuksellisia tietoja sai ainoastaan käsitellä. Näin riskin todennäköisyyttä voitiin pienentää entisestään tai jopa poistaa riski melkein kokonaan.

Henkilötietoriskit

Tietosuojalainsäädäntö edellyttää ainoastaan henkilötietoriskien kartoittamista ja niihin varautumista. Henkilötietoon liittyvästä riskistä on kyse aina silloin, kun riskin toteutuminen vaikuttaa jollain tavalla henkilöiden oikeuksiin tai vapauksiin (oppaan alusta mainitut kolme asiaa: kotirauha, kunnia ja oikeus yksityiselämään). Rekisterinpitäjänä jokaisen yrityksen on lisäksi varmistuttava siitä, että:

- yrityksessä käsitellään vain käyttötarkoitukseen liittyviä olennaisia henkilötietoja
- tietoja käsitellään läpinäkyvästi ja lain mukaan
- tiedot ovat oikeita ja paikkansa pitäviä
- tietoja ei säilytetä tarpeettoman pitkään
- tiedot eivät ole sellaisten tahojen saatavilla, joille ne eivät kuulu
- yritys kykenee osoittamaan myös jälkikäteen, että näitä periaatteita on noudatettu

Henkilötietoriskit ovat riskejä, jotka kohdistuvat näihin vaatimuksiin yrityksen näkökulmasta. Dokumentoitu ja kirjallinen riskienhallintatyö on avainasemassa siinä, että yritys voi myös osoittaa noudattaneensa vaatimuksia.

Riskienhallinta käytännössä

Kuten aiemmin oppaassa todettiin, voi riskienhallintaan käyttää mitä tahansa menetelmää, kunhan muistaa, että käsitellyssä ovat nyt vain henkilötietoriskit. **Jos asiassa alkuun pääsy tuntuu vaikealta, eikä mikään menetelmä ole tuttu, voi riskienhallinnassa käyttää apuna lomaketta 4.**

Käytännössä melkein kaikki riskit liittyvät näihin asioihin:

- henkilötieto katoaa tai ei ole käytettävissä
- henkilötieto vääristyy
- henkilötieto joutuu asiattomien tietoon

Riskienhallinnassa olennaista on näiden syiden ja seurausten tunnistaminen, joten lomake 4 toimii pohjana näiden asioiden pohdinnalle.

Lomakkeelle saattaa kertyä myös paljon epäolennaista tai epätodennäköistä asiaa, mutta sillä ei ole väliä. Pääasia on, että riskien tunnistamistyön tekee huolellisesti ja kirjallisesti monia eri vaihtoehtoja pohtien. Kannattaa myös pohtia, onko jokin asioista jo tapahtunut, mitkä olivat sen syyt ja mihin se johti. Apuna tässä työssä voi käyttää muita työntekijöitä tai vaikka saman alan yrittäjiä. Toki toteutuneista riskeistä puhuminen on ikävää, mutta kaikille niitä on sattunut. Pääasia on, että virheistä oppii.

Riskit kannattaa ehdottomasti myös arvottaa jollain tavalla. Tämä helpottaa sen arviointia, mihin riskeistä keskitytään ja mihin ei. Arvottamiseen ei ole mitään oikeaa tapaa. Yksinkertaisimmillaan sen voi tehdä vaikkapa värikynillä, jolloin korkean riskin asiat voi kirjata punaisella ja matalan riskin asiat vihreällä. Erilaisia muita asteikkoja voi myös käyttää. Väliä ei ole sillä, arvotetaanko riskit yhdestä kolmeen, yhdestä viiteen tai yhdestä kymmeneen. Arvottamalla saa kuitenkin käsityksen siitä kannattaako yksittäiseen riskiin keskittyä heti vai joskus myöhemmin.

Tietosuojan vaikutustenarviointi

Tietosuojan vaikutustenarviointi ei ole osa riskienhallintaa, mutta koska se liittyy siihen ja kyseessä on hyvin samankaltainen menettely, esitellään se tässä vaiheessa.

Tietosuojan vaikutustenarviointi on lainsäädännön mukaan pakko tehdä, jos henkilötietojen käsittely voi aiheuttaa korkean riskin henkilöille, joiden tietoja käsitellään. Tietosuojaviranomainen ylläpitää lisäksi

luetteloita käsittelytoimista, joiden yhteydessä on tehtävä tietosuojan vaikutustenarviointi tai mitkä ovat sellaisia toimia, joiden yhteydessä sitä ei tarvita [7.]. Lisäksi jossain muissakin lainsäädönnöissä voidaan vaatia sellaisen tekemistä.

On hyvin mahdollista, että yrityksellä ei ole sellaisia käsittelytoimia, jotka edellyttäisivät tietosuojan vaikutustenarviointia. Vaikutustenarviointi on kuitenkin hyvä työväline riskienarvioinnin lisänä ja kannattaa miettiä sen käyttämistä etenkin, jos epäilee henkilötietojen käsittelyyn liittyvän riskejä, eikä ole varma niiden vaikutuksista tai suuruudesta.

Vaikutustenarviointia on hyvä miettiä myös silloin, kun aloittaa uudenlaisia käsittelytoimia tai on esimerkiksi ostamassa tietojärjestelmää tai ohjelmistoa, jossa on tarkoitus käsitellä henkilötietoja.

Tietosuojan vaikutustenarviointiin ei ole mitään määrämuotoista prosessia tai lain edellyttämää muotovaatimusta. Vaikutustenarvioinnin keskeisenä lähtökohtana on se, että yritys arvioi seuraavia asioita:

- kuvaa suunnitellut käsittelytoimet ja käsittelyn tarkoitukset hyvin
- arvioi käsittelytoimien tarpeellisuuden ja oikeasuhteisuuden tarkoituksiin nähden
- arvioi rekisteröityjen oikeuksia ja vapauksia koskevat riskit
- suunnittelee toimenpiteet riskeihin varautumiseksi

Myös tietosuojalvatuutettu on julkaissut ohjeita vaikutustenarvioinnin tekemiseksi nettisivuillaan. Samoin tietosuojatyöryhmä WP29 on julkaissut dokumentin nimeltä: "*Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää "liittyykö käsittelyyn todennäköisesti" asetuksessa (EU) 2016/679 tarkoitettu "korkea riski"* [8.]. Jos riskiarvioissa päätyy siihen tulokseen, että jotkin käsittelytoimet voivat aiheuttaa korkean riskin henkilöille, joiden tietoja käsitellään, kannattaa tutustua näihin ohjeisiin tarkemmin.

Hyvinvointikeidas Maijan riskienarviointi

Maija päätti viedä projektin loppuun asiakkaidensa tietojen kanssa. Juha ja Janita toimivat asiakaspalvelutilanteissa usein, joten hän otti heidät mukaan työhön. Yhdessä he tekivät arvioita erilaisista riskien mahdollisuuksista ja täyttivät lomakkeen 4. He myös päättivät tehdä toimenpiteitä riskien välttämiseksi.

Maija merkitsi lomakkeelle tärkeimmät ja heti tehtävät toimenpiteet punaisella, vähemmän tärkeät tai kiireettömät mustalla ja jo tehdyt toimenpiteet vihreällä. Valmis riskikartta, lomake 4, näytti Maijan yrityksessä seuraavan sivun kaltaiselta.

Tehdyt toimenpiteet kannattaa kirjata ylös, koska sillä tavoin täyttyy myös näiden asioiden osoitusvelvollisuus. Jos asioita kertyy lomakkeelle paljon, voi osan asioista siirtää omalle dokumentilleen ja jättää vähemmän tärkeät näihin lomakkeisiin. Laki ei sano mitään siitä, kuinka arviointi pitää tehdä, kunhan sen vaan tekee.

Jos yrityksessä käsitellään jotain hyvin arkaluonteista tietoa, kuten potilastietoja, voi olla tarpeen tehdä riskiarviot perusteellisemmin ja katselmoida ympäristöä tarkemmin. Sitä varten oppaan liitteenä on myös lomake 5.

Lomake 4 (Hyvinvointikeidas Maija)

Tapahtuma	Riskin syyt	Riskin seuraukset	Keinot vaikuttaa
Henkilötietoa joutuu vääriin käsiin Lähetetään asiakastietoja väärälle vastaanottajalle Joku kuulee asiakkaan tietoja vastaanotossa Ulkopuolinen pääsee verkkolevyasemalle	Sähköpostiohjelman osoitteen automaattinen täydennys Postitetaan jotain väärään osoitteeseen Keskustellaan asiakas-tiedoista muiden kuullen Tunnusten kalastelu	Asiakas ei saa viestiä / väärä ihminen saa sen. Muut kuulevat mahdollisesti arkaluonteista tietoa asiakkaasta VAKAVA! Kaikki terveystieto verkkolevyasemalla	Arkaluontoisia tietoja ei laiteta sähköpostilla, että riski pysyy pienenä, ohje... Päivitetään tietojen käsittelyohjeet... Otetaan käyttöön kaksitasoinen tunnistautuminen Juhalle, Janitalle ja Maijalle...
Henkilötieto ei ole saatavilla Haittaohjelma tuhoaa tai lukitsee tiedot Verkkoyhteys ei toimi Tulipalo tuhoaa paperiarkistot	Virustorjuntaohjelma puuttuu Virustorjuntaohjelma ei päivity Modeemi rikkoutuu tai kaapeli poikki Menetetään sopimukset	Tiedot voivat hävitä kokonaan tai lopullisesti Ei vakava, aina yhteyden saa vaikka puhelimen kautta – ei toimenpiteitä Asiakastieto ja maksutieto vaarantuu	Ostetaan koneisiin aina virustorjunta (tehdään jo) Siirrytään keskitettyyn ja valvottuun virustorjuntaan Tarkistetaan kiinteistön paloilmoittimet ja skannataan tärkeät tiedot
Henkilötieto vääristyy Tieto tallennetaan väärin Asiakas ei kerro osoitteenmuutoksesta	Ei tarkisteta tiedon oikeellisuutta	Asiakasta ei tavoiteta Asiakkaan tietoja menee vanhaan osoitteeseen (..asiakkaille ei tosin postiteta mitään, elleivät he pyydä sitä, joten pieni riski)	Tarkistetaan oikeat yhteystiedot aina kun niitä tarvitaan Tarkistetaan sopimusten uusimisvaiheessa aina henkilötiedot uudestaan ja tehdään tästä ohje

6. Tietojen siirrot ja sopimukset käsittelijöiden kanssa

Henkilötietojen käsittelyn määritelmä on hyvin laaja. Siitä johtuen se pitää sisällään monia sellaisia toimia, joita ei tulisi aina ajatelleeksi. Tässä kohtaa palataan hieman käsittelyn määritelmään niiltä osin kuin lainsäädännössä on nimetty henkilötietojen käsittelyksi henkilötietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville.

Aina, kun sopimussuhteessa siirretään henkilötietoa jollekin toiselle, on siitä oltava sopimus [9.]. Tämä on tietysti selvä asia silloin, kun konkreettisesti henkilötietoja siirretään vaikkapa viestintätoimistolle markkinointikampanjaa varten.

Moni ei tule kuitenkaan ajatelleeksi, että henkilötietoja tulee asetettua saataville myös silloin, kun toisen osapuolen ei ole välttämättä tarkoitus tehdä tiedoilla mitään. Esimerkiksi ulkoistettujen tilitoimistopalveluiden, IT-palveluiden ja ohjelmistovuokrauspalveluiden yhteydessä palveluntarjoajalla saattaa olla pääsy yrityksen henkilötietoihin ja se tekee heistä yrityksen henkilötietojen käsittelijän.

Mistä sopimus?

Monet toimialat ovat tehneet jäsenistölleen valmiita sopimusmalleja ja sopimusehtoja henkilötietojen käsittelystä. Ne ovat usein lakimiesten laatimia ja pitävät sisällään kaiken olennaisen informaation. Esimerkiksi taloushallintoliitto on julkaissut tällaiset tilitoimistoilleen ja kirjanpitäjilleen. Myös IT-alalla monet IT-palveluiden tarjoajat käyttävät esimerkiksi IT2018 -sopimusehtoja ja erityisesti niiden *Erityisehtoja henkilötietojen käsittelystä* -liitettä. Suurimmilla toimijoilla, kuten esimerkiksi Googlella ja Microsoftilla, on käytössään julkiset sopimusehdot, jotka he ovat toimittaneet palveluidensa käyttäjille. Näin ehdot ovat käytännössä kaikille samat.

Myös omalla toimiallalla voi olla tällaisiä sopimusmalleja ja -ehtoja jo käytössä, joten kannattaa asiasta kysyä, jos kuuluu johonkin toimialajärjestöön. Suomen Yrittäjät ovat myös julkaisseet kaikille jäsenilleen Asiakirjapankissa sopimuspohjia, jopa kolmella eri kielellä [10.]. Myös palveluntarjoajilla saattaa olla valmiita sopimuksia käytössä. Suositeltavaa on kuitenkin käyttää yleisesti käytössä olevia ja useiden toimijoiden hyväksymiä ja käyttämiä mallisopimuspohjia.

Viime aikoina monet tahot ovat myös lähettäneet omia sopimusehotuksia kumppaneilleen. Tällaiset sopimukset kannattaa lukea huolellisesti läpi, jotta saa käsityksen siitä, mihin ne velvoittavat yritystä. Pääsääntöisesti yhdistysten ja liittojen jäsenilleen laatimat yleispohjat ovat melko luotettavia, mutta jos kyse ei ole tällaisesta ja sopimusehdotus epäilyttää, kannattaa ehdottomasti kysyä apua asiantuntijalta.

Mistä pitää sopia?

Lainsäädännön näkökulmasta käsittelijään kohdistuu tiettyjä vaatimuksia, joista on sopimuksella sovittava. Oppaan tarkoitus on herättää ajattelemaan ja kysymään, onko omassa yrityksessä riittävät sopimukset tehty. Yksityiskohtaisemmissa kysymyksissä kannattaa kääntyä asiantuntijoiden tai toimialajärjestöjen neuvontapalveluiden suuntaan.

Tästä kuitenkin pääosa sopimusvaatimuksista:

1. **Käsittelijä saa käsitellä henkilötietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaan.**
   Jos käsittelijä tekee henkilötiedoilla jotain muuta kuin on sovittu, siirtyy rekisterinpitäjän vastuu käsittelijälle ja hänen on hoidettava sen mukaiset velvoitteet kuntoon. Kannattaa siis sopia vähintään siitä, mihin käsittelijä saa henkilötietoja käyttää ja missä laajuudessa. Ohjeistus on syytä olla kirjallisena sopimuksella.

2. **Käsittelijä vastaa siitä, että kaikki henkilötietoja hänen alaisuudessaan käsittelevät henkilöt ovat salassapitovelvollisia rekisterinpitäjän heille luovuttamista henkilötiedoista.**
   Tämä velvoite on jo laissa, mutta esimerkiksi poikkeuksellisessa henkilötietojen käsittelytapauksissa voi olla syytä edellyttää sopimuksella tätä velvoitetta käsittelijältä erikseen.

3. **Käsittelijä on velvollinen suojaamaan henkilötiedot.**
   Joskus voi olla tarpeen edellyttää käsittelijältä erityisiä suojaamiskeinoja, jos käsitellään esimerkiksi hyvin arkaluonteisia tietoja. Käsittelyn suojaamisesta ja esimerkiksi toimintatavoista henkilötietojen tietoturvapoikkeamien osalta on hyvä sopia.

4. **Henkilötietojen käsittelijä ei saa käyttää toista henkilötietojen käsittelijää ilman erillistä tai yleistä rekisterinpitäjän kirjallista lupaa.**
   Tänä päivänä on kuitenkin tavallista, että alihankkija käyttää vaikka ohjelmistoa, jota se vuokraa edelleen joltain muulta. Silloin voi olla tarpeen antaa käsittelijälle oikeus käyttää toista käsittelijää siinä laajuudessa kuin mitä käsittelystä on kohdassa 1 mainittu.

5. **Käsittelijä on velvollinen avustamaan rekisterinpitäjää rekisteröityjen oikeuksien käyttämisessä.**
   Joskus tästä voi olla seurauksena myös kustannuksia ja se, miten kustannukset halutaan jakaa, riippuu sopimussuhteesta ja palvelusta, josta sopimuksella on sovittu. Ainakin kustannusten jakautumisesta on siis hyvä sopia.

6. **Kannattaa sopia siitä, mitä henkilötiedoille tapahtuu, kun sopimus päättyy tai käsittely muuten lakkaa.**
   Yleisesti sovitaan joko tietojen palauttamisesta rekisterinpitäjälle tai niiden turvallisesta poistamisesta.

7. **Rekisterinpitäjällä on enemmän toimivaltuuksia käsittelijään nähden kuin aiemmin.**
   Rekisterinpitäjänä toimivalla yrityksellä on esimerkiksi oikeus tarkastaa käsittelijän toiminta, jos se epäilee käsittelijän poikkeavan ohjeistuksesta tai epäilee käsittelyssä olevan laiminlyöntejä. Tällaisten tarkastusten suorittamisajankohdat, ennakkoilmoitukset ja kustannusten jakautuminen on hyvä sopia yhdessä.

Tietojen siirrot EU-alueen ulkopuolelle

EU-kansalaisten tietoja ei saa siirtää unionin ulkopuolelle ilman, että henkilötietojen suoja on jollain tavalla varmistettu. Tähän on olemassa muutamia tapoja, joita noudattamalla siirron voi kuitenkin tehdä. Pienissä yrityksissä tällaiseen tilanteeseen harvoin joudutaan, joten siksi tässä oppaassa käsitellään vain tyypillisimmät pienten yritysten tilanteet.

Jos liiketoiminta on sen luonteista, että syystä tai toisesta joutuu siirtämään suuria määriä henkilötietoja EU-alueen ulkopuolelle, on syytä tutustua tietosuoja-asetuksen artikloihin 44 - 49 huolellisesti ja etsiä lisätietoja siirtojen lainmukaisuudesta [11.]. Hyvin tavallista on kuitenkin näin pilvipalveluiden aikakaudella, että tietoja siirtyy ympäri maailmaa - jopa melkein huomaamatta.

Tietoja voi aina siirtää vapaasti EU-alueella maiden rajojen yli. Unionin alueen ulkopuolelle niitä voi siirtää muutamassa tapauksessa. Suurempien yhtiöiden kanssa toimiessa ongelmia harvemmin esiintyy. Microsoft, Google, suurimmat operaattorit ja vastaavat ovat joutuneet hoitamaan asiansa jo kuntoon joko siirtämällä asiakkaidensa käsiteltävän henkilötiedon Eurooppaan tai laatimalla sen kaltaiset sopimukset ja käytännöt, että siirrot ovat laillisia. Monet eurooppalaisille asiakkaille palveluja tarjoavat pienemmätkin yhtiöt ovat asiansa jo hoitaneet. Olennaista on tässä vaiheessa selvittää, millä tavalla asiat on hoidettu. Rekisterinpitäjänä pieni yritys joutuu kantamaan saman vastuun kuin muutkin yritykset.

Pienissä yrityksissä tyypillinen tilanne on se, että käytetään jotain pilvipalveluna hankittua tietojärjestelmää, joka sattuu sijaitsemaan EU-alueen

ulkopuolella. Koska pienten yritysten neuvotteluvara on usein aika hankala isompiin yhtiöihin nähden, kannattaa ennen palveluiden hankintaa tarkistaa, että kohdemaa on Euroopan komission hyväksymä kohdemaa. Jos komissio on tehnyt päätöksen kohdemaan tietosuojan riittävyydestä, voidaan siirto sen perusteella sallia. Komissio ylläpitää luetteloa hyväksytyistä kohdemaista ja päivittää luetteloa nettisivuillaan sitä mukaan, kun listaan tulee muutoksia. Maat julkaistaan myös Euroopan unionin virallisessa lehdessä.

Melko usein tietojen kohdemaa on Yhdysvallat, jonka osalta on eräänlainen erityisjärjestely. Sitä kutsutaan Privacy Shield -järjestelyksi ja siinä olennaista on se, että järjestelyissä mukana olevalla yhtiöllä on Yhdysvaltain kauppaministeriön (Federal Trade Commission) hyväksyntä. Järjestelyyn mukaan hakevat yhtiöt joutuvat suorittamaan auditoinnin, jolla ne esittävät tietosuojansa tason olevan riittävän hyvä. Lista on Yhdysvaltain kauppaministeriön sivuilla julkinen ja kenellä tahansa on mahdollisuus tarkistaa, mitä yhtiöitä listalla on ja miten pitkään auditointi on voimassa.

Keinoja henkilötietojen siirtoon on muitakin, mutta usein ne lisäävät pienissä yrityksissä kohtuuttomasti hallinnollista työtä ja vaativat erityisiä sopimusmenettelyjä sekä mahdollisesti lakipalveluita, joihin harvoin on rahaa tai aikaa. Kun tietojärjestelmien ja palveluiden hankinnat suunnittelee siten, että kohtuuttomia toimia ei tarvita, on toiminta usein helpompaa. Tärkeää on kuitenkin muistaa, että muitakin vaihtoehtoja on, jos niille on tarvetta.

Hyvinvointikeidas Maijan sopimustilanne

Oppaan 4. osassa oli lomake 2 ja 3, joihin Maija koosti henkilötietojoukkojaan ja henkilötietojen virtoja. Lomakkeessa 2 oli kohdat **Käsittelijät** ja **Henkilötietojen siirrot Eta-alueen ulkopuolelle**, joihin palataan tässä vaiheessa:

Käsittelijät	*Tilitoimisto (sopimuskumppani), palveli Mailchimp (sähköpostimarkkinointi/uut*
Henkilötietojen siirrot Eta-alueen ulkopuolelle	*Henkilötietoja ei siirretä ETA-alueen u nimeltä Mailchimp, jonka postituslistat järjestely ja Yhdysvaltain liittovaltion k d/b/a MailChimp).*

Tietojoukkoja (ryhmiä) kootessaan Maija selvitti ja teki muistiinpanot, ketä henkilötietojen käsittelyyn osallistui. Esimerkiksi asiakkaiden laskutustiedon käsittelyyn osallistui myös Hyvinvointikeidas Maijan tilitoimisto, jonka vastuulla oli kirjanpito. Näin ollen Maijan oli tehtävä sopimus henkilötietojen käsittelystä tilitoimiston kanssa. Tilitoimistolta Maija kuuli, että heidän ohjelmistonsa oli ylläpidossa muualla kuin tilitoimistolla itsellään. Tämän ohjelmiston ylläpitäjän kanssa Maijan ei kuitenkaan tarvinnut tehdä sopimusta, sillä hänellä ei ollut suoraa sopimussuhdetta kyseiseen ohjelmiston ylläpitäjään. Sopimussuhteet olivat tässä kuvatun kaltaiset:

Hyvinvointikeidas Maija (rekisterinpitäjä) → **Tilitoimisto** → **Ohjelmiston ylläpitäjä**

Näin ollen Maijan ei tarvinut tehdä sopimusta henkilötietojen käsittelystä enää tilitoimiston sopimuskumppanin kanssa, vaan tilitoimisto vastasi henkilötietojen käsittelysopimuksista omiin käsittelijöihinsä nähden. Maijan piti kuitenkin huomioida hänen ja tilitoimiston välisellä sopimuksella erityisesti tämän 6. osan *Mistä pitää sopia?* -luvussa esitellyt kohdat 2. ja 4. Maijan oli siis velvoitettava tilitoimistoa käyttämään käsittelijöitä, jotka sitoutuvat Maijan henkilötietojen käsittelyn salassapitoon. Lisäksi oli hyvä kirjata ylös, että tilitoimistolla oli lupa Maijan palveluiden tuottamiseen liittyen käyttää myös muita käsittelijöitä siinä laajuudessa kuin palveluiden toimittaminen edellyttäisi.

Tilitoimiston kanssa sopimus oli mutkatonta muodostaa. Maija sai kuulla tilitoimistolta jo hyvissä ajoin, että he käyttivät taloushallintoliiton TAL2018 -sopimusehtoja, joissa oli jo huomioitu henkilötietojen käsittelyyn liittyvät asiat. Maija oli muutenkin saanut tilitoimistolta jo hyviä ohjeita henkilötietojen käsittelyyn liittyen esimerkiksi palkanmaksutietojen ja sairaslomatodistusten käsittelyyn, joten Maija uskoi, että tilitoimistolla olivat asiat kunnossa ja riittävät tiedot henkilötietojen käsittelystä uuden lainsäädännön mukaan. Maija varasi palaverin tilitoimiston asiakasvastaavan kanssa ja ehdot käytiin vielä yhdessä läpi ja tarkistettiin, että ne sopivat kummallekin.

IT-tuen kanssa asiat menivät yhtä helposti. Heidän IT-tukensa oli ratkaissut asian siten, että he olivat ottaneet käyttöön IT2018 -sopimusehdot, joissa oli liite IT2018 EHK (Erityisehtoja henkilötietojen käsittelystä). IT-tuen kanssa varattiin myös palaveri ja tarkistettiin, että sopimusehdot sopivat molemmille ja sopimuksen luonteeseen, joka heillä oli käytössä. Samalla huomattiin, että koko sopimuksessa oli muitakin vanhentuneita asioita, joten sopimus

saatiin ajan tasalle kaikilta osin.

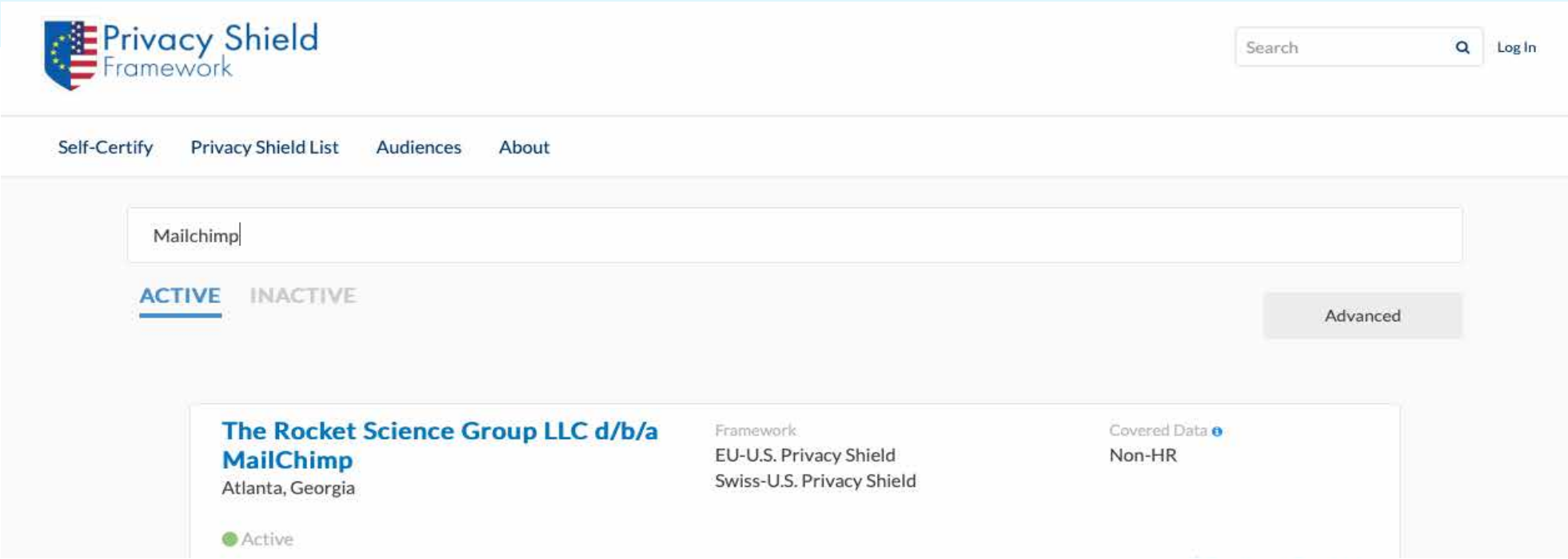
Maijalla oli henkilötietoja myös muualla. Asiakkaiden uutiskirjeet ja palvelutiedotteet lähetettiin Mailchimp -nimisellä ohjelmalla, jonka ylläpitäjä ja palvelut toteutettiin Yhdysvalloista käsin. Mailchimp oli ratkaissut henkilötietojen käsittelyyn liittyvät asiat siten, että he olivat vieneet tarvittavat muutokset suoraan yleisiin toimitusehtoihin, jolloin erillistä sopimusta heidän kanssaan ei tarvinnut tehdä. Maijan tarvitsi vain tarkistaa, että sopimusehdot olivat kohtuulliset hänen käsittelemien henkilötietojen näkökulmasta.

Henkilötietojen siirrot Hyvinvointikeidas Maijalla

Maijan postituslistat eivät sisältäneet kovin paljon tietoa, lähinnä nimiä ja sähköpostiosoitteita. Joka tapauksessa ne sisälsivät henkilötietoja, jolloin Maijan oli selvitettävä tietojen siirron lainmukaisuus EU-alueen ulkopuolelle.

Koska Yhdysvaltoja koski EU-US Privacy Shield -järjestely, Maija päätti tarkistaa, onko kyseisellä yrityksellä voimassa oleva auditointi. Maija muisti, että lista oli julkinen Yhdysvaltain kauppaministeriön (Federal Trade Commission, FTC) sivuilla, joten hän laittoi netin hakukoneeseen sanat “ftc privacy shield list”. Lista löytyi ensimmäisten hakutulosten joukosta ja sivuilla olevaan hakukenttään Maija kirjoitti “Mailchimp”. Sivu näytti Mailchimpin tulokset heti aktiivisten auditointien joukossa. Yrityksen nimeä klikkaamalla Maija sai vielä tarkempia tietoja.

Maijaa kiinnosti kuitenkin eniten se, että kaikki oli Mailchimpin osalta kunnossa ja lainmukaisuusperuste henkilötietojen siirrolle oli olemassa.



7. Rekisteröityjen oikeudet

Kaikkein olennaisinta rekisteröityjen eli luonnollisten henkilöiden oikeuksien toteutumisen näkökulmasta on tietosuoja-asetuksen viides artikla, avoimuuden ja läpinäkyvyyden toteutuminen henkilötietojen käsittelyssä.

Ihmiset myös luottavat paremmin tietojen käsittelijään, joka avoimesti ja rehellisesti kertoo, mitä heidän henkilötiedoillaan tehdään. Ja, jotta yrityksen edustajana ja rekisterinpitäjänä voi rehellisesti kertoa muille, mitä tietoa heistä käsittellään, kannattaa tehdä oppaan 3. osassa mainittu tietojen siivousurakka.

Monille yrityksille kertyy asiakkaista ja henkilöstöstä paljon tietoa. Suurin osa tästä tiedosta on tarpeellista vain vähän aikaa, mutta tiedoilla on silti tapana kertyä yrityksen tietovarastoihin. Osa tiedoista saattaa olla jo alkuperäisestä asiayhteydestä irrotettuna tai yhdistettynä muuhun kertyneeseen tietomassaan. Silloin tieto on myös kyseenalaista ja voi johtaa jopa täysin vääränlaisiin tulkintoihin ihmisistä ja heidän asioistaan.

Mitä oikeuksia rekisteröidyllä on?

Rekisteröidyillä eli ihmisillä, joiden tietoja käsittellään, on useita oikeuksia omiin tietoihinsa. Tässä käydään niistä valtaosa läpi, mutta kovin syvälle ei oikeuksien osalta kuitenkaan mennä. Tärkeintä on, että tietää perusasiat ja pystyy toimimaan oikein esimerkiksi rekisteröityjen käyttöoikeuspyyntöjen kanssa (tämän osan seuraavassa luvussa on kerrottu lisää käyttöoikeuspyynnöstä).

Tässä tärkeimmät rekisteröidyn oikeudet, jotka koskevat pieniä yrityksiä:

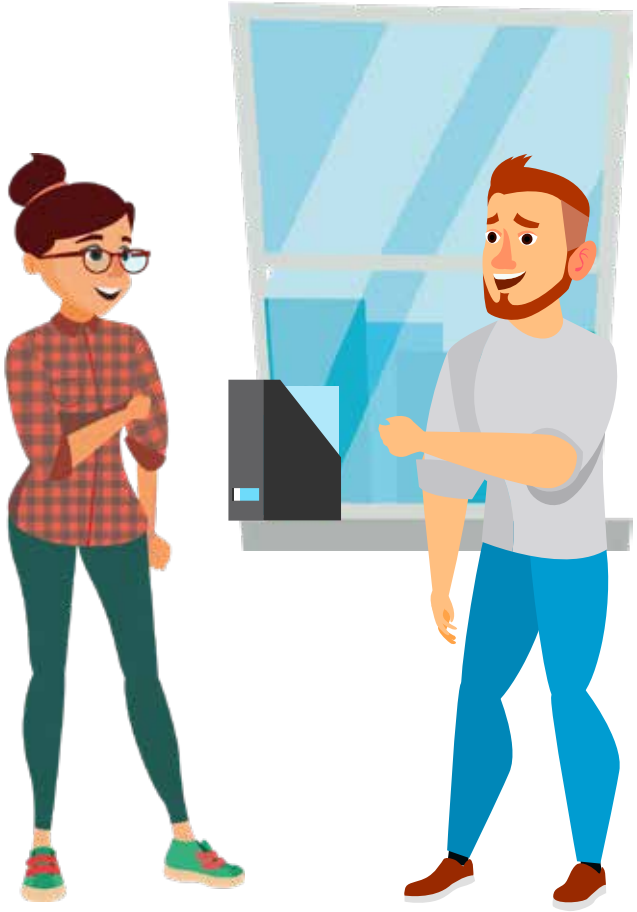
Oikeus saada pääsy henkilötietoihin *(12.)*

Jokaisella on oikeus tutustua hänestä tallennettuihin ja häneen liitettävissä oleviin tietoihin. Pääsy tietoihin voidaan järjestää vaikkapa suoraan asiakkaan oman käyttöliittymän tai järjestelmään kirjautumisen kautta. Se voidaan toteuttaa myös siten, että tiedot toimitetaan henkilölle itselleen helposti luettavassa muodossa. Jos tietojen saanti tietojärjestelmistä on erityisen hankalaa, voidaan ne perustellusti esitellä asiakkaalle paikan päällä suoraan tietokoneelta. On kuitenkin muistettava, että mahdollisia potilastietoja luovutettaessa pitäisi paikalla olla terveydenhuollon ammattihenkilö, jolle voidaan esittää tarkentavia kysymyksiä tietojen sisällöstä.

Oikeus tietojen oikaisemiseen *(13.)*

Jokaisella on oikeus pyytää korjausta virheellisiin tai puutteellisiin tietoihin. Tämä on tavallaan itsestään selvää, koska tuskin kukaan haluaa säilyttää vanhentunutta laskutusosoitetta.

Poikkeus tähän voi olla tilanne, jossa aiemmin toimitettu tieto on jollain tavalla olennainen esimerkiksi sopimukseen tai toimitukseen liittyen (rahtikirjat, toimitussopimukset, ym). Tällöin tietoa, joka on olennaista sen hetkisen tapahtuman todentamiseksi, ei pidä lähteä oikaisemaan.



Oikeus tietojen poistamiseen *(14.)*

Tätä oikeutta kutsutaan myös oikeudeksi tulla unohdetuksi. Tätä oikeutta on mahdollista käyttää esimerkiksi seuraavissa tilanteissa:

- henkilö peruuttaa henkilötietojen käsittelyn suostumuksen (esimerkiksi uutiskirjetilauksen), eikä käsittelylle ole muuta perustetta
- henkilö vastustaa tietojensa käsittelyä eikä

käsittelyn jatkamiselle ole muuta perustetta, esimerkiksi markkinointiviestinnän osalta
- henkilön tietojen käsittelylle ei ole lain vaatimaa perustetta ja käsittelyn tarve on lakannut. Tällainen tieto pitäisi poistaa säilytyksen rajoittamisen ja minimointi-periaatteen mukaan ilman henkilön pyyntöäkin.

Samoin kuin edellisenkin oikeuden kohdalla, on tässäkin selvitettävä, miksi tietoa säilytetään. Jos asiakkaan lasku- ja toimitustietoja tai työntekijän Kela-korvauspäätöksiä tarvitaan kirjanpitoaineiston säilytysvelvollisuuden vuoksi, ne on yrityksestä myös löydyttävä. Silloin niille on myös lakisääteinen säilytysperuste. Kannattaa aina selvittää tarkkaan, missä laajuudessa tietojen säilyttäminen on olennaista. Vaikka laista johtuvista syistä joutuu säilyttämään työntekijän työtodistusta työsuhteen päättymisen jälkeen, ei varmasti ole esimerkiksi oikeutta säilyttää vanhoja muistioita kehityskeskusteluista tai työntekijän lähiomaisten tietoja.

Oikeus käsittelyn rajoittamiseen *(15.)*

Henkilöillä on oikeus pyytää henkilötietojen käsittelyn rajoittamista esimerkiksi tilanteissa, joissa epäillään henkilötietojen käsittelyn lainmukaisuutta tai henkilö on vastustanut henkilötietojensa käsittelyä, mutta asioiden selvittäminen on vielä kesken.

Oikeus tietojen siirrettävyyteen *(16.)*

Henkilöillä on oikeus saada häntä koskevat tiedot yleisesti käytössä olevassa ja koneellisesti luettavassa muodossa eli sähköisenä. Oikeus koskee henkilötietoja, joita käsitellään sopimukseen tai suostumukseen perustuen ja käsittely on automaattista.

Vastustamisoikeus *(17.)*

Kaikilla on oikeus vastustaa tietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseen vedoten, jos rekisterinpitäjä käsittelee tietoja yleiseen etuun (tilastointi tai tutkimus) tai rekisterinpitäjän omaan oikeutettuun etuun perustuen (esimerkiksi suoramarkkinointi). Jos yritys ei voi perustella, että sillä olisi huomattavan tärkeä ja perusteltu syy tietojen käsittelyyn, on henkilötietojen käsittely lopetettava. Suoramarkkinointitarkoituksiin tai siihen liittyvään profilointiin liittyvä käsittely on aina lopetettava henkilön sellaista vastustaessa.

Automatisoidut yksittäispäätökset ja profilointi *(18.)*

Jokaisella on oikeus vastustaa henkilötietojensa automaattista käsittelyä, jolla olisi suoria vaikutuksia häneen. Lisäksi jokaisella on oikeus olla joutumatta profiloinnin kohteeksi.

Rekisteröidyn oikeuksien käyttöpyynnön toteuttaminen

Kannattaa muistaa, että mitkään oikeuksista eivät ole absoluuttisia. Ne ovat aina suhteessa toisten oikeuksiin ja vapauksiin sekä yrityksen oikeuksiin ja velvollisuuksiin nähden. Jos asiakkaan vaatima tieto sisältää tietoja myös kolmannesta osapuolesta, pitää olla varma, ettei tiedon luovuttaminen voi vahingoittaa kolmatta osapuolta. Myös viestinnän luottamuksellisuus on huomioitava. Jos asiakas pyytää työntekijän kanssa käymäänsä kirjeenvaihtoa, ei voida kajota työntekijän sähköpostiin ilman hänen lupaansa.

Pääsääntöisesti kannattaa aina pohtia rekisteröidyn oikeuksien käyttöpyynnön tullessa asioita seuraavassa järjestyksessä:

- Miten laajasti rekisteröity tietoja vaatii?
- Mitä tietosuojalainsäädäntö ja muu lainsäädäntö asiasta sanoo (työlainsäädäntö, vuosilomalaki, laki työterveyshuollon järjestämisestä, kirjanpitolainsäädäntö, verottajan ohjeet, yms.)?
- Sisältääkö luovutettava tieto tietoja kolmansista osapuolista ja mitkä ovat heidän oikeutensa?
- Onko luovutettavien tietojen laajuutta tarpeen sovittaa ja millä perusteella?
- Voiko tietojen joutuminen vääriin käsiin vaikuttaa jotenkin henkilöön, jos kysyjä onkin joku muu? Onko pyynnön esittäjä tarpeen tunnistaa jotenkin, esimerkiksi ajokortista paikan päällä tai sähköisellä allekirjoituksella verkossa?

Käyttöpyyntöihin on vastattava kuukauden kuluessa pyynnön saapumisesta. Sitä varten on hyvä kirjata jonkinlainen ohje ja suunnitelma jo etukäteen, sillä muuten ensimmäisen pyynnön tullessa se saattaa olla työlästä. Pienissä yrityksissä tieto on usein vain muutamassa eri paikassa ja nyt, kun tietojen säilytyspaikat on jo kuvattuna, on varsin helppoa kirjata ylös perusasiat. Kannattaa kirjata dokumentille vastaukset ainakin näihin kysymyksiin:

- Kuka yrityksessä käsittelee käyttöpyynnöt?
- Miten pyynnön esittäjä tunnistetaan, jos se on tarpeen?
- Kuka kerää tiedot ja mihin muotoon?
- Miten ne toimitetaan?
- Mihin tietopyynnöt kirjataan, jos niitä tarvitaan vaikkapa tietosuojaviranomaiselle?

Rekisteröityjen oikeudet Hyvinvointikeidas Maijalla

Maijan mielestä oli tärkeää, että henkilökunta osaisi toimia oikein sellaisessa tilanteessa, jossa esimerkiksi asiakkaalta tulisi tietojen käyttöpyyntö. Maija halusi, että tilanteessa toteutuisivat rekisteröidyn oikeudet ja lisäksi hän halusi, ettei pyyntöön vastattaessa vaarannetttaisi kenenkään sivullisen tai yrityksen tietoja. Tämän vuoksi Maija aloitti ohjeiden kirjaamisesta.

Rekisteröityjen oikeuksista keskusteltiin myös henkilökunnan viikkopalaverissa, mutta kukaan ei muistanut, että asiakkaat olisivat koskaan aikaisemmin vaatineet oikeuksiaan. Roni kuitenkin muisti, että hän oli tehnyt juuri osoitteenmuutoksen yhden kuntosaliasiakkaan tietoihin, koska asiakas oli muuttanut. Siinä oli kyse rekisteröidyn oikeudesta omien tietojen oikaisuun.

Ronja taas muisti, että eräs asiakas oli joskus soittanut ja pyytänyt laskun viitettä ja toimitusosoitetta, koska ei ollut mielestään saanut alkuperäistä laskua. Siinä oli myös kyse asiakkaan oikeudesta tarkistaa omia tietojaan.

Keskustelun edetessä Maija päätyi kirjaamaan ohjeeseen: *"Tavanomaiset henkilötietojen käsittelyyn liittyvät pyynnöt, kuten osoitteenmuutokset, asiakkaan palveluiden voimassaolon tarkistaminen hänelle itselleen, laskujen uudelleenlähetykset sekä suppeat tietopyynnöt voidaan hoitaa suoraan puhelimitse, jos ei ole kyse arkaluonteisista tai maksuliikenteeseen liittyvistä tiedoista.*

Sopimusmuutokset ja maksuihin vaikuttavat asiat sekä asiakkaiden ohjelmiin ja terveystietoihin liittyvät muutokset ja tietopyynnöt on aina tehtävä paikan päällä, jotta asiakas voidaan tunnistaa.

Kaikki laajat tietopyynnöt ja sellaiset, joiden luovuttamisesta ei olla varmoja, ohjataan Maijalle ja hän vastaa pyyntöihin vastaamisesta. Asiakkaalta otetaan soittopyyntö ja yhteystiedot sekä luvataan, että häneen ollaan yhteydessä."

Viimeinen lause oli järkevä, koska Maija oli ainut, jolla oli pääsy kaikkeen tietoon. Muulla henkilökunnalla oli tehtävän ja toimenkuvan mukaan rajatut oikeudet tietoihin, joten kaikkien tietojen luovuttaminen ei olisi edes mahdollista. Maijalla oli myös paras tieto tietosuojalainsäädännöstä, koska oli tutustunut tietosuojaan ja tehnyt töitä tämän oppaan parissa.

Maijalle jäi rekisteröityjen informoinnista vielä monia selvitettäviä asioita, joten hän alkoi selvitellä niitä yksi kerrallaan. Tässä työssä hän käytti apuna lomaketta 6, josta löytyi hyvä muistilista.

8. Rekisteröidyille informointi

Rekisteröidyille informointi liittyy olennaisesti rekisteröidyn oikeuksiin saada oikeaa tietoa henkilötietojensa käsittelystä. Monet yritykset ovat ymmärtäneet tämän niin, että koko informointi olisi hoidettu päivittämällä vanhat, henkilötietolain aikaiset, rekisteriselosteet.

Olemassa olevia rekisteriselosteita voi käyttää työn pohjana, mutta tietosuoja-asetus edellyttää, että henkilötietojen käsittelyyn liittyvä tieto on toimitettava aikaisempaa laajempana rekisteröidylle, hänen sitä pyytäessä. Pyydetty tieto on myös toimitettava rekisteröidylle kirjallisena ja yhteen dokumenttiin koottuna.

Nykyinen tietosuojalainsäädäntö ei enää edellytä erityistä määrämuotoista rekisteriselostetta. Lainsäädännön kannalta ei ole merkitystä, miksi informointiin liittyviä lomakkeita tai nettisivuja kutsuu. Merkitystä on sillä, mitä tietoa niistä löytyy [19.]. Käyttöön on vakiintunut tietosuojalausunto tai tietosuojaseloste. Osa yrityksistä on otsikoinut tiedotteensa yleisesti "Henkilötietojen käsittely Yritys X:ssä".

Kaikki olennaiset selvitettävät ja rekisteröidyille toimitettavat tiedot löytyvät kootusti tietosuojavaltuutetun nettisivuilta taulukosta nimeltä "*Informointivelvoitteen edellyttämät tiedot*" [20.]. Taulukosta nähdään, että aiemmat selvitykset ja kartoitukset toimivat hyvänä apuna tässä vaiheessa. Osaan kohdista on todennäköisesti joutunut miettimään vastauksia jo aiemmin, mutta vastaavan taulukon julkaiseminen oman yrityksen nettisivuilla ei ole kuitenkaan lainsäädännön hengen mukaista.

Selkeys ja käyttäjäkeskeisyys

Mahdollisimman kattavan ja yksityiskohtaisen tiedon toimittamisen ja selkeyden välillä on selkeä ristiriita. Jos kaiken asetuksen vaatiman henkilötietojen käsittelyyn liittyvän informaation toimittaa kerralla, yhdessä pitkässä selosteessa, se ei täytä rekisteröidyn suuntaan lainsäädännön selkeyden vaatimusta. Ihmisten pitää saada tiedot helposti ymmärrettävässä muodossa ja selkeällä kielellä esitettynä. Mielellään siten, että tietosuojaselosteen rakenne etenee yleisestä asiasta yksityiskohtaisempaan tietoon. Ensimmäisellä tasolla olisi aina informoitava vähintään:

- yksityiskohdat henkilötietojen käsittelyn käyttötarkoituksista
- rekisterinpitäjän identiteetti
- kuvaus rekisteröityjen oikeuksista ja niiden käyttämisestä

Tämän jälkeen yksityiskohtaisemman tiedon pitäisi olla esitettynä siten, että rekisteröity itse löytää yksityiskohdat hänen näkökulmastaan ymmärrettävällä tavalla. Tämän voi toteuttaa esimerkiksi yksinkertaisella nettisivunavigaatiolla, infolaatikoilla, väliotsikoinnilla tai muulla tarkoituksenmukaisella tavalla. Olennaista on se, että informaatio toimitetaan käyttäjälähtöisesti.

Jos kyse on henkilötietoa keräävästä teknisestä laitteesta, jossa ei ole näyttöä, perinteinen nettisivu ei ole välttämättä tarkoituksenmukaisin paikka informoida rekisteröityä eikä se välttämättä täytä asetuksen vaatimuksia. Ylipäätään nettisivuilla olevan rekisteriselosteen olemassaolo ei ole välttämättä riittävä keino informoida rekisteröityjä, vaan rekisterinpitäjältä edellytetään aktiivisia toimia tietojen toimittamiseen rekisteröidyille.

Lähtökohtana viestinnässä laki pitää käyttäjäkeskeisyyttä (ei juridista tai lain muotovaatimusta) keskeisenä asiana. Rekisterinpitäjä on itse velvoitettu arvioimaan ja tarvittaessa käyttämään esimerkiksi kyselytutkimuksia tai käyttäjäpaneeleita sen arvioinnissa, mikä on tarkoituksenmukaisin informaatiokanava sekä viestintätapa ja kieli. Tarvittaessa voi kysyä suoraan asiakkailta, että kaipaavatko he jotain lisätietoja henkilötietojensa käsittelystä.

Erityisesti rekisterinpitäjän vastuulla on tunnistaa, millainen on hänen keskiverto käyttäjäkohderyhmä ja miten viestintä heille pitää toteuttaa. Esimerkiksi viestiessä tietyn alan ammattilaisille voi kieli olla monimutkaisempaa, mutta jos käyttäjäkohderyhmään kuuluu esimerkiksi vanhuksia tai lapsia, pitää ilmaisussa olla erityisen tarkka. Ja, vaikka suostumus lapsen henkilötietojen käsittelyyn olisi saatu huoltajalta, on lapsella itsellään silti oikeus saada sama tieto henkilötietojen käsittelyyn liittyen kuin muillakin rekisteröidyillä.

Tietosuojaselosteen juridinen "kapulakieli" ei siis täytä asetuksen selkeyden vaatimusta – ellei sitten viestitä lakimiesliiton jäsentiedotteessa. Myös kaikenlaiset ympäripyöreydet ovat vältettävien ilmaisujen listalla. Sellaisia ovat esimerkiksi: "tietojasi saatetaan käyttää", "voidaan käyttää", "usein" tai "mahdollisesti".

Rekisterinpitäjän tulee olla yksiselitteinen siinä,

miten rekisteröidyn henkilötietoja todella käsitellään ja mihin tarkoituksiin. Myös lause- ja kappalerakenteet tulee olla selkeitä ja ymmärrettäviä.

Monissa päivitetyissä rekisteriselosteissa näkee edelleen huonoja esimerkkejä:

- "*Saatamme käyttää henkilötietojasi uusien palveluiden kehittämiseen.*"
  Tämä on huono, koska esimerkissä ei kerrota, mitä palvelut ovat ja kuinka henkilötiedot auttavat kehittämään niitä.
- "*Saatamme käyttää henkilötietojasi tutkimuksellisiin tarkoituksiin.*"
  Tämä on huono, koska lauseesta ei käy ilmi, millaiseen tutkimukseen tällä viitataan.
- "*Käytämme henkilötietojasi personoitujen palveluiden toimittamiseen.*"
  Tämä on huono, koska lauseesta ei käy ilmi, mitä personointi tarkoittaa tai mihin sillä viitataan.

Jos rekisterinpitäjän tiedossa on jo etukäteen, että käsittelyyn voi sisältyä riskejä tai yllätyksiä rekisteröityjen suuntaan, on näistä tiedotettava etukäteen avoimesti. Rekisteröidyltä ei voida olettaa, että hän itse tunnistaisi häneen kohdistuvia riskejä. Niinpä suositeltavaa on liittää mukaan esimerkiksi tietosuojan vaikutustenarvioinnissa kirjatut havainnot rekisteröidyille olennaisista riskeistä.

Läpinäkyvyys koskettaa koko käsittelyketjun elinkaarta - ei vain tietojen keruuta. Aina, jos selosteisiin tulee olennaisia muutoksia, on rekisteröityjä informoitava.

Epäolennaisia muutoksia ovat esimerkiksi kieliasun muutokset, ilmaisuun ja kirjoitusvirheisiin liittyvät korjaukset.

Aktiivisesti informoitavia muutoksia ovat esimerkiksi:

- muutokset henkilötietojen käsittelyn vaikutuksista rekisteröityihin
- rekisteröidyn kannalta yllättävät ja odottamattomat vaikutukset
- henkilötietojen käsittelyn käyttötarkoituksen muuttuminen
- rekisterinpitäjän muuttuminen tai vaihtuminen
- kaikki rekisteröityjen oikeuksien käyttöön liittyvät muutokset

Muutosten yhteydessä täytyy aina miettiä, osaako asiakas itse käydä nettisivuilla toteamassa muutokset vai olisiko syytä informoida asiakkaita esimerkiksi sähköpostijakelulla tai yrityksen ilmoitustaululla.

Seloste käsittelytoimista

Kun rekisteriselosteeseen on saatu koottua rekisteröidyille informoitavat tiedot, täytyy huolehtia, että selosteesta löytyy myös henkilötietojen käsittelytoimet. Lainsäädäntö edellyttää käsittelytoimista informoitointia organisaatioilta, jotka työllistävät yli 250 henkilöä tai organisaatioilta, joissa:

- henkilötietojen käsittely aiheuttaa riskin rekisteröityjen oikeuksille ja vapauksille tai...
- henkilötietojen käsittely ei ole satunnaista tai...
- henkilötietojen käsittely kohdistuu erityistietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin henkiltötietoihin.

Jokainen työnantaja käsittelee säännönmukaisesti vähintään työntekijöidensä tietoja. Lisäksi työntekijöiden osalta käsitellään myös erityistietoryhmiä, kuten esimerkiksi terveystietoja työterveyslainsäädännön ja kirjanpitosäännösten takia. Tämä tarkoittaa sitä, että jokaisella organisaatiolla pitäisi olla seloste käsittelytoimista vähintään työntekijöidensä henkilötietojen osalta. Asiakkaiden ja muiden sidosryhmien osalta on syytä tarkistaa, soveltuuko jokin kolmesta poikkeustilanteesta heihin [21.].

Käsittelytoimien kirjaaminen ei ole kovin työlästä, jos on toiminut oppaan ohjeiden mukaan. Tähän mennessä on kerätty jo tarvittavat tiedot käsiteltävistä henkilötiedoista.

Tietosuojavaltuutettu on julkaissut nettisivuillaan ladattavat esimerkkipohjat selosteesta sekä rekisterinpitäjille että käsittelijöille [22.]. Tosin hyvin pienissä yrityksissä selosteita voi hiukan tästä vielä yksinkertaistaa.

Selostetyypit

Edellisissä luvuissa puhuttiin kolmesta erilaisesta selosteesta:

- Informointivelvoitteen edellyttämät tiedot
- Tietosuojaseloste tai -lausunto
- Seloste käsittelytoimista

Näiden suhdetta toisiinsa sekä pääasiallista käyttötarkoitusta voidaan kuvata seuraavan kuvan kaltaisesti:

Yrityksen koko henkilötietojen käsittely kootusti omaan käyttöön ja viranomaisen pyynnöstä toimitettava heille.

- Ei julkinen

Nämä ovat tarkoitettu henkilöille, joiden tietoja käsitellään. Jakelu tehdään siten, että se tavoittaa kohderyhmän mahdollisimman hyvin.
Selkeä kielenkäyttö ja riittävän perusteellisia.

- Julkinen ja aktiivisesti tiedotettu

Tarkoitettu henkilöille, joiden tietoja käsitellään.
Täydellinen koonti kaikesta käsittelystä.

- Tätä ei useimmiten julkaista, mutta toimitettava henkilön sitä pyytäessä.

Rekisteröityjen informointi Hyvinvointikeidas Maijalla

Maija päätti hoitaa informoinnin asiakkaiden osalta kahdella eri tavalla, koska asiakkaat jakautuvat pääsääntöisesti kahteen ryhmään palvelujen hankinnan suhteen. Kuntosaliasiakkaat olivat tottuneet tilaamaan ja maksamaan internetin kautta salikorttinsa, joten tilauslomakkeelle ja nettisivuille lisättiin linkit tietosuojaselosteisiin. Tilauslomakkeelle Maija lisäsi myös lauseen, jossa kerrottiin tietojen keruun tapahtuvan kuntosalipalvelujen tuottamiseksi asiakkaalle ja laskutusta varten. Lomakkeelle tuli myös Maijan yrityksen yhteystiedot ja ohjeet, mistä löytyisi lisää tietoja. Lisäksi tilauslomakkeelle tuli erikseen rastitettava kohta, jossa kysyttiin, onko asiakas kiinnostunut tarjouksista tai kuntosaliharrastukseen liittyvistä tuotteista, joita Hyvinvointikeidas Maija tarjoaa. Näin Maija sai samalla kerättyä tarvittavat suostumukset markkinointiin.

Nettisivujen rekisteriselosteelle Maija kokosi kaiken olennaisen tiedon kerättävistä henkilötiedoista, henkilötietojen käsittelyn tarkoituksista, lainmukaisuusperusteista ja siitä, miten asiakas saisi halutessaan lisätietoja tietosuojasta. Selosteeseen Maija kokosi myös PT- ja fysioterapia-asiakkaita koskevat tiedot, sillä olisi mahdollista, että joku asiakkaista etsisi tätä tietoa yrityksen nettisivuilta.

Maija oli käytännössä huomannut, että fysioterapia-asiakkaat tulivat usein joko lähetteellä suoraan paikan päälle tai varasivat puhelimella ajan. Monet eivät käyneet nettisivuilla muutoin kuin katsomassa yhteystiedot, joten nettiasiointi ei ollut heille tuttua tai kuulunut palvelun normaaliin käyttöön. Siksi Maija päätti liittää osan perustiedoista asiakkaiden perustietolomakkeelle eli käytännössä hän lisäsi lomakkeelle samat asiat kuin nettisivun tilauslomakkeelle.

Maija pohti myös laajemman tietosuojaselosteen tulostamista asiakkaille. Maija kuitenkin epäili tulostamisen olevan vain ajan ja paperin tuhlausta, koska asiakkaille ei jäänyt muutenkaan mitään omaa sopimuskappaletta tai säilytettävää dokumentaatiota. Maija päätti kuitenkin tulostaa laajemman fysioterapia-asiakkaille kohdennetun tietosuojaselosteen asiakkaiden odotustilan ilmoitustaululle. Varmuuden vuoksi hän myös tulosti muutaman kappaleen tietosuojaselosteita Juhan ja oman työpöytänsä laatikkoon, jos asiakas haluaisi sellaisen itselleen.

Sähköisen version, tietosuojavaltuutetun lomakkeen pohjalta ("*Informointivelvoitteen edellyttämät tiedot*") tehdyistä, laajemmista kartoituksista Maija tallensi verkkolevylle Tietosuoja -kansioon, johon hän kokosi myös kaikki tekemänsä selosteet.

Tietosuoja -kansioon tuli myös seloste henkilötietojen käsittelytoimista työntekijöiden osalta, joten jokainen työntekijä pystyi tarvittaessa hakemaan tietoja kansiosta. Näin työntekijöiden tietoja koskevia selosteita ei tarvinut julkaista missään muualla.

9. Poikkeamien hallinta ja ilmoitusvelvollisuus

Tietosuojapoikkeamilla tarkoitetaan tapahtumia, jotka vaarantavat jollain tavalla henkilöiden vapaudet ja oikeudet, kuten yksityisyyden, kotirauhan tai kunnian. Poikkeama voi olla myös tapahtuma, jonka vuoksi yritys ei syystä tai toisesta täytä lakisääteisiä velvoitteitaan. Tällaisia tapahtumia voivat olla esimerkiksi vahingossa väärälle asiakkaalle lähetetyt toista henkilöä koskevat tiedot, asiakastietoja sisältävän USB-tikun katoaminen, haittaohjelman pääsy tietokoneille, henkilötietojen joutuminen sivullisten tietoon huolimattoman hävittämisen kautta tai virheellinen tai puutteellinen tiedottaminen henkilötietojen käsittelyn käyttötarkoituksista.

Usein ensimmäisenä mieleen tulee, että ainoa henkilötietoon liittyvä riski on sen joutuminen vääriin käsiin. Olennaista on kuitenkin, että tietoturvaloukkauksina ei pidetä vain luottamuksellisuuteen kohdistuvia loukkauksia. Loukkaukset on arvioitava aina luottamuksellisuuden, eheyden ja saatavuuden ongelmina. Eli myös se, että tiedot eivät ole saatavilla, kun niitä tarvitaan, voi aiheuttaa mahdollisen riskin rekisteröidyille.

Olennaista on, että jokainen yritys pyrkii tunnistamaan ja seuraamaan tällaisia tapahtumia omassa ympäristössään. Rekisterinpitäjän vastuulla on tuntea toimintansa ja sen aiheuttamat riskit, joten pelkkä riskienarviointi ei riitä. Omaa toimintaa on myös seurattava ja osoitusvelvollisuuden vuoksi tapahtumat on kirjattava ylös. Niiden perusteella on myös suunniteltava parempia käytäntöjä, etteivät ongelmat toistu.

Teknisten poikkeamien seuranta on usein yksinkertaista. Virustorjuntaohjelmat, palomuurit ja erilaiset valvontaohjelmat tuottavat usein pienten yritysten toimintaan riittävän informaation ja takaavat monesti tarvittavan suojaustason. Tekniikka on kuitenkin vasta puolet asiasta, sillä myös ihmisten toiminnasta johtuvia poikkeamia on kyettävä tunnistamaan ja estämään. Siksi on tärkeää, että pienissäkin yrityksissä turvallisuuteen suhtaudutaan heti alusta asti yhdessä tehtynä kehitysprojektina - ei syyllisten etsintätyönä. Mitä enemmän työntekijät luottavat työnantajaansa ja mitä enemmän asia koetaan yhteisenä projektina, sen paremmat ovat tulokset.

Ongelmista, virheistä ja poikkeamista on siis opittava keskustelemaan rakentavasti viimeistään tässä vaiheessa. Apuna voi käyttää kuukausipalavereita, tavoitekeskusteluja tai vaikka ihan erikseen tätä varten varattuja keskustelutilaisuuksia, joissa pyritään arvioimaan oman toiminnan turvallisuutta.

Poikkeamiin varautumisen toinen puoli tekniikan lisäksi ovat laissa mainitut organisatoriset toimenpiteet [23.], eli miten ihmisten toiminnan kautta voidaan varautua poikkeamiin. Näitä keinoja ovat usein perehdytys tietojärjestelmien käyttöön, niiden käyttöohjeet sekä ohjeet siitä, miten henkilötietoja yrityksessä saa käsitellä - oli kyse sitten ohjelmistoista tai papereista.

Vanha sanonta kuuluu, että ihminen on tietoturvan heikoin lenkki. Tämä tarkoittaa myös sitä, että parhaimmillaan osaava ihminen on tietoturvan vahvin lenkki.

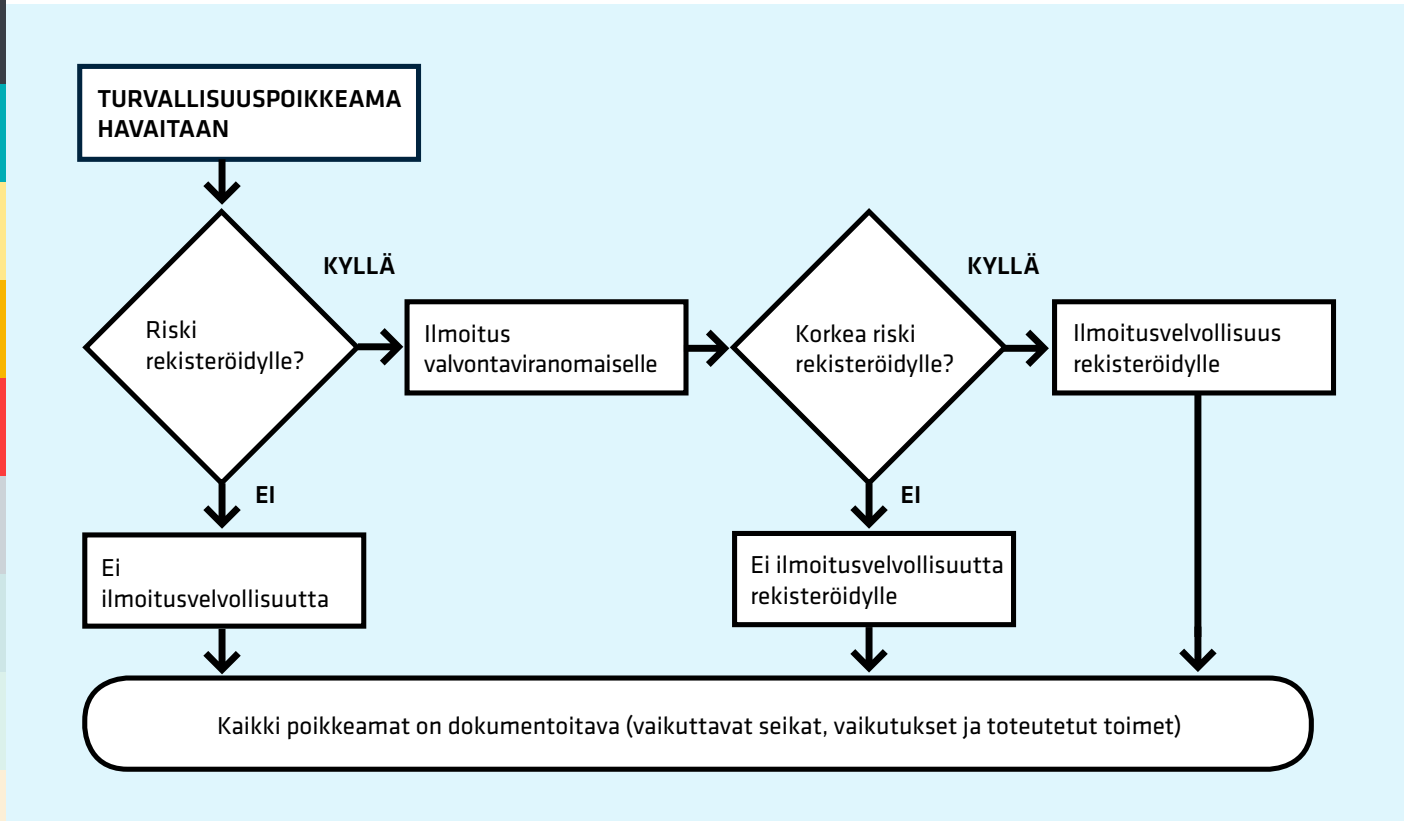
Ilmoitusvelvollisuus

Jokaisen yrityksen ja rekisterinpitäjän on kyettävä jatkossa tekemään ilmoitus viranomaiselle aina, kun henkilötietojen käsittelyyn liittyvä poikkeama aiheuttaa riskin luonnollisille henkilöille. Ilmoituksen tekemiseen on aikaa 72 tuntia sen havaitsemisesta. Jos poikkeama aiheuttaa korkean riskin, on siitä tiedotettava myös henkilöitä suoraan [24.]. Tietosuojavaltuutetun sivuilla on tätä varten tarkempia ohjeita sekä lomake ilmoituksen tekemiseen [25.]. Mutta ennen kuin voi tehdä lain vaatimaa ilmoitusta, on poikkeamat kyettävä havaitsemaan. Vasta sen jälkeen voidaan tehdä arvio siitä, vaatiiko poikkeama ilmoitusta vai ei.

Poikkeaman havaitsemisen jälkeen on ensin määriteltävä, aiheuttaako poikkeama riskin rekisteröidylle. Jos aiheuttaa, on ilmoitus tehtävä vähintään valvontaviranomaiselle. Jos poikkeama aiheuttaa korkean riskin rekisteröidylle, on siitä ilmoitettava valvontaviranomaisten lisäksi rekisteröidylle itselleen.

Kaikki poikkeamat on joka tapauksessa aina kirjattava ylös. Tämä siksi, että riskien ajallinen ulottuvuus on kyettävä huomioimaan. Jos esimerkiksi salattu tietokanta joutuu vääriin käsiin, mutta salausavaimet ovat turvassa, ei tapahtuma ehkä aiheuta riskiä. Jos salausavaimet taas joutuvat puolen vuoden kuluttua vääriin käsiin ilman tietokannan menetystä, on aiempi tapahtuma kyettävä huomioimaan, koska ne yhdessä aiheuttavat ilmoitusvelvollisuuden.

Ilmoitusvelvollisuuden arvioinnin voi esittää tämän sivun kaltaisella kuvalla.



Riskiä arvioitaessa (ei riski, riski vai korkea riski) on otettava huomioon:

- **Riskin tyyppi**
  Onko kyseessä tiedon luottamuksellisuuteen, eheyteen vai saatavuuteen liittyvä riski? Esimerkiksi potilashistorian joutumisella vääriin käsiin on erilaiset seuraukset kuin sen tuhoutumisella.

- **Henkilötiedon luonne, arkaluontoisuus ja laajuus**
  Nimi ja osoite voivat olla jonkun osalta jo muullakin tavoin julkista tieto, mutta tilanne on eri henkilöllä, joka on joutunut hankkimaan turvakiellon henkeen ja terveyteen kohdistuvien uhkauksien vuoksi. Pelkkä syntymäaika ei vielä riitä identiteettivarkauteen, mutta henkilötunnus, asuinpaikka, valokuva ja perhesuhdetiedot voivat johtaa sitten jo toisenlaiseen tilanteeseen.
  Sanomalehden tilaajatiedon paljastuminen ei välttämättä aiheuta rekisteröidylle riskiä, mutta jakelun keskeytymistieto loma-aikana voi rikollisissa käsissä aiheuttaa omaisuusriskin.

- **Henkilöiden tunnistettavuus**
  Jos henkilötiedoista on vaikea tunnistaa yksilöä

riittävän tarkasti, ovat seuraukset rekisteröidyille silloin epätodennäköisempiä.

- **Seurausten vaikutukset**
  Taloudelliset ongelmat, identiteettivarkaus, julkinen nöyryytys tai vahinko maineelle ovat pahempia kuin potentiaalinen väärin perustein kohdistuva suoramarkkinointi. Etenkin, jos poikkeama koskee haavoittuvassa asemassa olevia kansalaisia, kuten vaikkapa lapsia ja vanhuksia. Toisaalta henkilötietojen vahingossa tapahtuva lähettäminen sopimus kumppanille (vaikkapa tilitoimistolle), jonka voi olettaa yhteistyössä haluavan tuhota tiedot, on eri asia kuin niiden joutuminen sellaiselle taholle, jolla voi olla intressi käyttää tietoa väärin.

- **Rekisteröidyn erityispiirteet**
  Jos poikkeama koskee haavoittuvassa asemassa olevia kansalaisia (lapset, vanhukset, jne.), joiden voi olla vaikea tai mahdoton vaikuttaa seurausten vakavuuteen tai puolustautua niiltä, voivat seuraukset olla pahemmat.

- **Rekisteröityjen lukumäärä**
  Mitä useampaa rekisteröityä poikkeama koskee, sen vakavampi se on. Silti vain yhden henkilön arkaluonteisten tietojen joutuminen vääriin käsiin voi olla suurempi riski kuin sadan henkilön nimiluettelon joutuminen julkiseksi.

- **Rekisterinpitäjän erityispiirteet**
  Poliittisten järjestöjen ja aatteellisten yhdistysten jäsenluettelo voi kertoa rekisteröidyistä julki jotain, jonka rekisteröity laskee kuuluvaksi yksityisyyden piiriin.

- **Muut yleiset tekijät**

Poikkeaman seurausten arvioinnissa kannattaa luottaa maalaisjärkeen. Jos kadotat asiakastilaisuuden osallistujalistan, jossa ei ole muuta kuin nimiä ja päivämäärä, ei tällä tiedolla todennäköisesti voi vahingoittaa ketään. Ja, aika spekulatiivista se olisi, vaikka tapahtumalista sisältäisi osallistujien ruoka-aineallergiatkin, vaikka se terveyteen liittyvää tietoa onkin.

Tapahtumat tulee aina ylös ja niihin on liitettävä perustelu, miksi ilmoitusta ei ole tehty. Näin voi jälkeenpäin osoittaa havainneensa ongelmat ja reagoineensa niihin. Tällä tavoin voi myös perustella, miksi ilmoitusta ei tehty. Jos asiaan myöhemmin palataan jonkun muun havainnon vuoksi, se on paljon parempi kuin omistaa yritys, joka ei edes tiedä, millaisia poikkeamia siellä tapahtuu. Tosiasia on se, että poikkeamia tapahtuu jokaisessa yrityksessä.

Tietosuojatyöryhmä on myös julkaissut erilaisia esimerkkejä tietosuojaluokkauksista [26.].

Tietosuojapoikkeamat Hyvinvointikeidas Maijalla

Maija lähti liikkeelle siitä, mistä se oli helpointa eli, mitä oli jo tapahtunut. Riskienarvioinnin yhteydessä tuli jo aiemmin esiin läheltä piti -tilanteita ja vähäisiä poikkeamia, jotka hän kokosi silloin itselleen muistiin. Hän myös varasi seuraavaan yhteiseen palaveriin puoli tuntia enemmän aikaa ja kävi tilanteet vielä uudestaan läpi kaikkien kanssa. Kuten tavallista, osalle oli tullut mieleen jo pari muutakin aikaisempaa tapahtumaa ja osa oli keksinyt tällä välin uusia potentiaalisia ongelmia. Maija kirjasi kaikki tilanteet ja poikkeamat ylös ja niiden osalta myös keskusteltiin tavoista, joilla voitaisiin estää niitä tapahtumasta.

Palaverin tarkoitus oli myös kertoa työntekijöille, miten pitää toimia, jos epäilee poikkeamaa. **Maija oli tehnyt itselleen tietosuojavaltuutetun ohjeiden perusteella lomakkeen 7 poikkeamia varten, jonka hän kävi läpi henkilöstön kanssa.** Koska lomake ei ollut kaikille ihan selvä, sovittiin yhdessä, että kaikki poikkeamat ilmoitettaisiin aina Maijalle. Maija vastaisi sitten lomakkeen täytöstä, lisätietojen selvittämisestä ja sen tallentamisesta.

Maijan mielestä oli tärkeää, että hän saisi tiedon kaikista mahdollisista poikkeamista, vaikka työntekijä ei aina sitä osaisi tarkkaan edes kuvata. Poikkeaman havaitsemisen jälkeen Maija voisi kuitenkin tehdä poikkeaman kuvauksen yhdessä työntekijänsä kanssa.

Maija korosti palaverissa vielä, että koska he tarjosivat asiakkailleen hyvinvointipalveluita, olisi heidän huolehdittava asiakkaiden hyvinvoinnista kokonaisuutena. Maija oli sitä mieltä, että tämä asia oli osa sitä työtä, jolla asiakkaiden luottamus ja hyvinvointi varmistettaisiin mahdollisimman kokonaisvaltaisesti. Virheiden tai ongelmien esille tuomista ei saanut nähdä kenenkään virheenä, vaan se oli asiakkaista ja toisista työntekijöistä huolehtimista.

10. Nettisivut ja evästeet

Evästeet, toiselta nimeltään cookiet, ovat pieniä tiedostoja, joita tallennetaan verkkosivustojen käyttäjien koneille heidän vieraillessaan verkkosivuilla. Moni pieni yritys käyttää näitä (joskus jopa tietämättään) tarjotessaan verkkosivuilla esimerkiksi chat -palveluita tai seuratessaan verkkosivuanalytiikkaa. Jos olet epävarma, miten omien nettisivujen laita on, kannattaa ottaa yhteyttä niiden tekijään.

Tietosuoja-asetuksessa ei mainita suoranaisesti evästeitä. Tietosuoja-asetus koskettaa kuitenkin yksityisyydensuojaa melko läheisesti ja puhuu muun muassa luonnollisten henkilöiden suostumuksesta heidän tietojensa käsittelyyn liittyen. Tietosuoja-asetus on niin sanottu yleislainsäädäntö, jota voidaan tarkentaa erityislainsäädännöllä.

Tällä hetkellä EU:ssa on valmisteilla uusi sähköisen viestinnän tietosuoja-asetus (asetus tunnetaan nimellä ePrivacy regulation) [27.]. Tämä on niin sanottu 'lex specialis' eli erityislainsäädäntö, joka tarkentaa yleislainsäädäntöä.

Sähköisen viestinnän tietosuoja-asetus puhuu suoraan evästeistä. Tämä asetus on kuitenkin vasta ehdotus, joten meidän on katsottava tarkemmin sen edeltäjää, sähköisen viestinnän tietosuojadirektiiviä. Tässä direktiivissä todetaan, että: *"...tilaajan tai käyttäjän päätelaitteelle tallennettujen tietojen käyttämiseen sallitaan ainoastaan sillä edellytyksellä, että kyseiselle tilaajalle tai käyttäjälle annetaan selkeät ja kattavat tiedot muun muassa käsittelyn tarkoituksesta...ja että hänelle annetaan oikeus kieltää tietojen käsittelystä vastaavaa tahoa suorittamasta tällaista käsittelyä."*

Ohjeistus evästeiden käyttöön Suomessa

Suomessa evästeiden käyttöä koskevaa ohjeistusta on antanut Traficom (ent. Viestintävirasto) [28.]. Suomessa ei toistaiseksi ole vaadittu mitään erityistä ponnahdusikkunaa tai hyväksyntämenettelyä evästeiden käytön yhteydessä. Evästeiden käytöstä on kuitenkin kerrottava verkkosivuilla siten, että käyttäjällä on mahdollisuus tutustua niiden käyttötarkoituksiin ja saada niistä lisätietoja. Viestintävirasto kertoo myös, että evästeistä ei tarvitse tiedottaa:

- jos niiden ainoana tarkoituksena on toteuttaa viestin välittäminen teknisesti
- jos niiden ainoana tarkoituksena on helpottaa palvelun käyttöä
- jos käyttäjä on pyytänyt evästeiden käyttöön perustuvaa palvelua (esimerkiksi verkkopankkipalvelut)

Yleisesti käytössä olevia toimintatapoja evästeiden käyttöön

Koska maailma ja lainsäädäntö sen mukana ovat muuttumassa, organisaatiot ovat jo valmistautumassa muutoksiin. Maailmalla on tällä hetkellä yleistynyt kolme tapaa ilmoittaa evästeistä, joista voidaan suositella käyttämään jotain vaihtoehtoa. Vähintään ainakin Viestintäviraston ohjeistuksen mukaista ensimmäistä tapaa.

1. **Evästetiedote**
   Tietosuojaselosteessa tai -lausunnossa oleva osa tai sitten sivustolla muuten selkeästi erillään oleva osio, joka kertoo käyttäjille, mihin evästeitä käytetään, miksi niitä käytetään, miten kauan niitä säilytetään ja millaisia keinoja käyttäjillä on vaikuttaa evästeiden hallintaan.

2. **Evästeiden hyväksyntätyökalu**
   Verkkosivustolle oleva erillinen työkalu, jonka linkki tai tunniste on jossain sivustolla näkyvissä, ja jonka avulla käyttäjä voi itse päättää, tallentaako sivusto evästeitä vai ei.

3. **Evästeilmoitus**
   Erillinen banneri tai pop-up -tiedote, joka sisältää ilmoituksen evästeiden käytöstä sisältäen linkit tarkempiin tietoihin ja mahdolliseen evästeiden hallinnan työkaluun. Ihannetilanteessa tällaisen tiedotteen häviäminen edellyttää käyttäjältä esimerkiksi "Hyväksyn evästeiden käytön" -painikkeen klikkaamista.

Kotimaan markkinoilla tulee käyttää vähintään ensimmäistä tapaa. Käytännöt ja direktiivin tulkinta vaihtelevat valtioittain. Jos yritys palvelee ulkomaisia asiakkaita, kannattaa tutustua kohdemaan tapaan toimia ja käyttää sen mukaan mahdollisesti muita käytäntöjä.

Evästekäytäntö Hyvinvointikeidas Maijalla

Maijan yrityksellä oli melko yksinkertaiset nettisivut. Hänen omasta mielestään siellä ei ollut muuta kuin yritysesittely kuvineen ja muutama palvelukuvaus sekä ulkopuoliselta toimijalta ostettu korttimaksupalvelu, jolla kuntosaliasiakkaat maksoivat salikorttinsa. Varmuuden vuoksi Maija soitti kuitenkin nettisivujen tekijälle ja yllättyi melkoisesti. Nettisivuilla oli verkkokauppa, josta löytyi kaikkien asiakkaiden ostohistoria alusta asti. Sen lisäksi siellä oli käyttäjätunnuksia ja salasanoja sekä asiakkaiden sinne itse tallentamia tietoja (valokuvia, liikuntaprofiilin kuvauksia, osoitteita, jne.). Verkkokauppa teki myös jatkuvaa analysointia siitä, mitä kukakin käyttäjä sivustolla klikkasi ehdottaakseen verkkokaupassa klikkausten perusteella sopivia ostoksia. Maijalla ei ollut nettisivuilla juuri tuotteita eikä hänellä siten ollut käyttöä tälle tiedolle, mutta siitä huolimatta näitä tietoja oli kerätty nettisivuilta alusta asti.

Tämä uusi tieto aiheutti sen, että asiakasrekisterien kuvauksiin ja tietovirtoihin oli lisättävä ihan uusi rekisterin osa; verkkokauppa. Samoin sen riskit oli arvioitava. Tämä oli tärkeää, koska verkkokaupan tiedot olivat periaatteessa koko ajan julkisessa verkossa, vaikka pääsy sinne oli varmistettu käyttäjätunnuksilla ja salasanoilla. Yksi unohtunut verkkokaupan päivitys voisi kuitenkin tällaisessa tapauksessa saattaa kaikki tiedot ulkopuolisten käsiin. Maija myös kuuli nettisivujen toimittajalta, että hän ei ollut ostanut ikinä päivityspalvelua nettisivuilleen, joten sivuston päivitykset olivat tekemättä ja tämä oli toimittajan mukaan jo aika suuri riski. Maija oli luullut, että kerran tehdyt nettisivut olisivat aina toimintakuntoiset ja turvalliset, mutta saikin kuulla, että julkisessa verkossa olevat palvelut vaativat usein jatkuvaa huolenpitoa. Maija pyysi heti tarjouksen nettisivujen päivityspalvelusta, koska ei osannut itse päivityksiä tehdä.

Toimittajan kanssa sovittiin myös, että sivustolle lisättäisiin ilmoitus evästeiden keruusta. Evästeilmoituksesta tuli hyvin yksinkertainen, koska Maijalla ei ollut asiakkaita ulkomailla. Sivustolle tultaessa selaimeen lisättiin ilmoitus, että sivusto kerää evästeitä vierailijoiden seurantaan ja lisäksi siihen lisättiin linkki, josta löytyisi tietosuojaseloste ja lisätietoja asiasta.

Maija pyysi nettisivujen tekijältä vielä kuvauksen koko sivuston tietoturvasta. Hän ei itse osannut tulkita tätä saamaansa tietoturvakuvausta, mutta IT-tuen tullessa käymään, hän kävi sen läpi heidän kanssaan. Näin hän sai kolmannen osapuolen arvion asiasta ja pystyi rekisterinpitäjänä olemaan varma siitä, että nettisivujen tietoturva olisi asianmukaisella tasolla.

Profilointi Hyvinvointikeidas Maijalla

Verkkokaupan ominaisuuksien paljastuminen toi Maijalle myös toisen huolenaiheen, jota hän ei ollut aiemmin joutunut miettimään. Verkkokauppa keräsi käyttäjistä heidän itse ilmoittamiaan tietoja, mutta myös ostokäyttäytymistietoja ja käyttäjien selailutietoja.

Maija tiesi, että pelkästään asiakkaiden luokittelu tai markkinointiviestin kohdentaminen iän tai asuinalueen perusteella ei ollut profilointia, mutta hänen nettisivujensa kautta kerrättiin tätä enemmän tietoa. Hän päätti selvittää, mitä profilointi tarkoittaa ja löysi tietosuojavaltuutetun toimiston nettisivuilta vastauksen: *"Profiloinnilla tarkoitetaan erityisesti työsuoritukseen, taloudellisen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin liittyvien piirteiden analysointia tai ennakointia."* [29.]

Ostokäyttäytymisessä sekä sivuston ja verkkokaupan selailuun liittyvässä seurannassa oli suurimmassa määrin kyse juuri henkilökohtaisten mieltymysten ja kiinnostusten kohteiden selvittämisestä. Se tapahtui automaattisesti järjestelmän toimesta, kohdistui suoraan tunnistettavissa olevaan henkilöön ja siinä arvioitiin henkilökohtaisia ominaisuuksia.

Lyhyellä aikavälillä kerättyjen tietojen osalta Maijan verkkokauppatiedot eivät kertoneet kovin paljon asiakkaista, koska verkkokaupan tuote- ja palveluvalikoima oli hyvin suppea. Pitkällä aikavälillä ja useiden ostotapahtumien kautta sieltä pystyi jo tekemään päätelmiä henkilön liikuntaprofiilista, aktiivisuudesta, tuotteisiin liittyvistä mieltymyksistä ja valintojen perusteella jopa mahdollisesti taloudellisesta tilanteesta. Niinpä Maija rajasi, että verkkokaupan osalta käyttäjien tietoja säilytettäisiin vain edellisen kalenterivuoden osalta. Näin tietoa olisi jatkossa vain kuluvalta kahdelta vuodelta eikä käyttäjille muodostuisi tunnistettavia profiileja. Mitä vähemmän tietoa olisi, sen vähemmän käyttäjistä voitaisiin päätellä.

Maijalla oli myös verkkokaupan tiedot reskontrassa, joten käyttäjien asioihin palaaminen onnistuisi joka tapauksessa vielä myöhemmin. Tarvittaessa hän myös voisi muodostaa asiakasprofiilit reskontran tietojen perusteella eikä tieto näin olisi netissä kaikkien saatavilla, jos verkkokauppaan joku murtautuisi.

Maija varmisti vielä nettisivujen toimittajalta, että verkkokaupan osalta olisi mahdollista kytkeä pois

päältä jonkun tietyn tunnuksen tai käyttäjän seurantatieto. Maija teki näin, koska hänen oli täytettävä kaksi asetuksen vaatimusta:

1. Profiloinnista kertominen selosteilla ja rekisteröityessä verkkokauppaan
2. Antaa käyttäjille mahdollisuus kieltäytyä profiloinnista heidän niin halutessaan

11. Sähköpostimarkkinointi

Suoramarkkinointi on asia, josta liikkuu eniten väärinkäsityksiä. Osa pelkää, ettei voi tehdä sitä enää ollenkaan ja osa on sitä mieltä, että sitä voi tehdä ihan miten haluaa. Kumpikaan näistä käsityksistä ei ole täysin oikein. Suoramarkkinointia saa toki tehdä edelleen, mutta sitä ei voi tehdä ihan miten haluaa. Käytännössä tapoja on kaksi [30.]:

1. Suostumukseen perustuva suoramarkkinointi
2. Oikeutetun edun perusteella tapahtuva suoramarkkinointi

Ensimmäinen on helppo. Riittää, että asianosainen itse rastittaa nettisivulla lomakkeen tai liittymiskaavakkeen suostumuskohdan (huomioitavaa on, että valmiiksi rastitettu ruutu ei käy, koska suostumus pitää olla itse annettu ja vapaaehtoinen). Suostumuksen jälkeen riittää, että säilyttää sähköisen tai paperisen suostumuslomakkeen. Näin voi markkinoida asiakkaalle palveluita, joita on ilmoittanut markkinoivansa suostumusta kerätessä. Suostumusta kerätessä on siis jo kerrottava, millaiseen ja mihin markkinointiin henkilö suostumuksensa antaa [31.].

Toinen on hiukan monimutkaisempi. Tietosuojaasetus sanoo suoramarkkinoinnin menevän elinkeinonharjoittajien oikeutetun edun piiriin, koska kyse on elinkeinon harjoittamisen vapaudesta ja markkinointi sen edistämistä. Mutta, kun käytetään oikeutettua etua, on yrittäjän vastuulla kyetä dokumentoidusti osoittamaan, että oikeutetun edun käyttäminen on juuri se sopivin ja paras vaihtoehto eikä rekisteröidyn omat oikeudet tai edut mene sen edelle. Oppaan 4. osassa mainittiin käsittelyn lainmukaisuusperusteesta ja tasapainotestistä. Käytännössä nämä tarkoittavat, että on tehtävä tasapainotesti edellä mainittujen asioiden osoittamiseksi.

Tasapainotestistä löytyy hyvät ohjeet tietosuojavaltuutetun sivuilta. Osoitusvelvollisuuden vuoksi testi on tehtävä ja dokumentoitava ennen suoramarkkinoinnin aloittamista.

Suoramarkkinointia ei kuitenkaan pidä sekoittaa normaaliin palvelutiedottamiseen. Asiakkaille voi huoletta tiedottaa aukioloaikojen muutoksista, palveluihin tai tuotteisiin liittyvistä ominaisuuksista, niiden muutoksista tai vaikka tuotteita täydentävistä lisäosista. Jos asiakkailla on sopimussuhde yritykseen ja heille kerrotaan tähän sopimukseen liittyvistä asioista, ei kyseessä ole markkinointi. Jos kuitenkin myy kampaamopalveluita, mutta samalla kertoo sopimusasiakkaille puolison yrityksen IT-tukipalveluista, kyse on markkinoinnista, koska asianmukaista suhdetta näiden palveluiden ja asiakkaidesi välillä ei ole.

Tasapainotesti

Tasapainostesti on vapaamuotoinen, mutta kirjallinen arviointi siitä, miten oikeutettu etu sopii henkilötietojen käsittelyn lainmukaisuusperusteeksi. Lisätietoja tästä on Tietosuojavaltuutetun sivuilla [32.], mutta lyhyesti Suomen viranomaisen mukaan testissä on kyse siitä, että arvioidaan seuraavat asiat:

1. Onko oikeutettu etu sopivin käsittelyperuste vai sopisiko jokin muu paremmin, esimerkiksi sopimussuhde tai suostumus?

2. Täyttyvätkö perusvaatimukset sen osalta, että etu on todella yksilöitävissä oleva, selkeä ja lainmukainen?

3. Onko henkilötietojen käsittely tarpeen edun saavuttamiseksi vai voitaisiinko samaan lopputulokseen päästä muutenkin?

4. Syrjäyttääkö etu todella rekisteröidyn edut ja oikeudet? Mitä hyötyä ja haittaa käsittelystä on?

5. Onhan kaikki mahdolliset tekniset ja organisatoriset tietoturvatoimet todella tehty rekisteröityjen oikeuksien ja vapauksien suojaamiseksi?

Tulee siis osoittaa toiminnan lainmukaisuus ja varmistaa avoimuus. On oltava valmis perustelemaan omat näkemykset ja neuvottelemaan niistä uusien näkökulmien tullessa esiin.

Suoramarkkinointi Hyvinvointikeidas Maijalla

Suoramarkkinointia varten oli aiemmin kerätty aina suostumus asiakkailta. Maijan kuultua, että hänellä olisi mahdollisuus markkinoida palveluitaan myös ilman suostumusta, ajatus tuntui houkuttelevalta. Niinpä hän teki tasapainotestin oikeutetun edun käyttämisestä. Etu piti nimetä, joten Maija nimesi sen näin: Elinkeinon harjoittamisen vapaus ja harjoittamansa elinkeinon edistäminen suoramarkkinoinnilla.

Maija juuttui kuitenkin tasapainotestin kohtiin 1. ja 3. (ks. edellinen sivu), koska hänellä oli jo suostumus niiltä, joille hän halusi markkinoida lisäpalveluita. Sopimusasiakkaille palvelutiedotteiden lähettämistä ei lasketa markkinoinniksi ja erilaisissa tapahtumissa ja tempauksissa kerättyjen ihmisten henkilötietojen osalta keruulomakkeessa pyydettiin jo suostumus suoramarkkinointia varten. Eli olemassa oleviin asiakkaisiin oli sopimussuhde (kohta 1) ja potentiaalisilta asiakkailta oli jo suostumus (kohta 3).

Lisäksi Maija pääsi jo markkinoinnin osalta samaan lopputulokseen kuin olisi päässyt oikeutetun edun käyttämisen myötä. Yritys on alusta asti käyttänyt markkinoinnissa paikallislehtien ilmoitusmainontaa, tapahtumamarkkinointia ja muita epäsuoria keinoja ja ne oli todettu hyvin toimiviksi. Maija ei loppujen lopuksi itsekään uskonut, että ihmiset innostuisivat, jos saisivat häneltä yllättäen ja pyytämättä postia.

Maija uskoi, että jos hän markkinoisi niille ihmisille, jotka olisivat oikeasti kiinnostuneita hänen palveluistaan, olisivat tulokset parempia kuin satunnaisilla massapostituksilla valikoimattomalle kohderyhmälle lähetyt markkinointisähköpostit. Postitusten teko olisi myös vaatinut työtä niiden suorittamiseen, eikä siihen aina löytynyt aikaa. Eikä siihen, että loukkaantuneet ihmiset kyselisivät, mistä heidän tietonsa olivat hankittu ja miksi heille lähetettiin posteja palveluista, joihin heillä ei ollut mitään yhteyttä.

Lopulta Maija totesi nykyisen käytännön parhaaksi ja unohti koko oikeutetun edun käyttämisen suoramarkkinoinnissa.

12. Tietosuojavastaava

Pienissä yrityksissä on harvoin lakisääteistä tarvetta nimetä tietosuojavastava. Toisaalta pientenkin yritysten toiminta voi olla sen kaltaista, että lain vaatimus täyttyy. Usein tällaisissa tapauksissa on kyse erikoisemmista toimialoista tai yritysmuodoista.

Joskus organisaatiot hyötyvät tietosuojavastaavan vapaaehtoisesta nimittämisestä. Erityisesti yrityksissä, joissa käsitellään asiakkaiden näkökulmasta arkaluonteista tietoa tai tietoa käsitellään tavalla, joka on epätavallinen, voi tietosuojavastaavan nimittäminen auttaa asiakkaiden luottamuksen vahvistamisessa.

Joillekin yrityksille tietosuojavastaavan nimittäminen on tärkeä osa yhteiskuntavastuun tai sosiaalisen vastuun osoittamisessa työntekijöille, asiakkaille ja yhteistyökumppaneille.

Toisilla kyse on paljon yksinkertaisemmasta asiasta. Tietosuoja-asetuksen velvoitteet koskevat jokaista yritystä ja organisaatiota, yhdistyksistä pörssiyhtiöihin, ja usein on helpompaa ja kustannustehokkaampaa antaa tehtävä jollekin, joka tietää mitä tehdä. Henkilön ei tarvitse olla tietosuojavastaava nimekkeeltään, mutta jokaisessa yrityksessä on hyvä olla joku, joka vastaa tietosuojan toteutumisesta sekä valvoo ja kehittää sitä.

Tietosuojavastaavan nimittäminen on organisaatiossa pakollista, jos [33.]:

- tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Lainsäädännössä voidaan vaatia tietosuojavastaavan nimittämistä myös muissa tilanteissa.

Tietosuojavastaavan pätevyys ja tehtävät

Lainsäädännössä mainitaan, että tietosuojavastaavaa nimitettäessä tulisi ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä, yleisestä tietosuoja-asetuksesta ja alan käytänteistä. Tietosuojavastaavalla tulisi myös olla valmiudet suorittaa lainsäädäntöön kirjatut tietosuojavastaavan tehtävät. Käytännössä mitään “minimitasoa” tai eksakteja rajoja ei ole, vaan on aina pohdittava sitä, mikä osaaminen on riittävää yrityksen toimintaan ja sen luonteeseen nähden.

Tietosuojavastaavan tehtävä on mm. [34.]:

- auttaa tietosuojalainsäädännön toteuttamisessa
- seurata tietosuojasääntöjen noudattamista ja tuoda esille havaitsemiaan puutteita
- raportoida johdolle sekä antaa tietoja ja neuvoja henkilötietoja käsitteleville työntekijöille
- toteuttaa tietosuojan vaikutustenarviointia ja avustaa siinä
- auttaa rekisteröityjä (työntekijöitä, kumppaneita ja asiakkaita) omien oikeuksien toteuttamisessa

Tietosuojavastaavan asiantuntemuksen tason on oltava suhteessa organisaation käsittelemien tietojen arkaluonteisuuteen, monimutkaisuuteen ja määrään. Tietosuojavastaavalla on hyvä olla käytössään myös asianmukaiset resurssit tehtäviensä hoitamiseen. Toimialan tuntemus on tarpeen, mutta usein tietosuojavastaava joutuu ottamaan kantaa niin käsittelytoimien toteutustapaan kuin yleisiin tietoturvaperiaatteisiin ja niiden toteutumiseen. Tietosuojavastaavalla on siis hyvä olla näkemystä myös riskienhallinnasta ja tietoturvallisuuden toteutuksista organisaatiossa.

Tietosuojavastaavalla on keskeinen asema yrityksen tietosuojakulttuurin vahvistamisessa ja yleisen tietosuoja-asetuksen olennaisten osien täytäntöönpanossa. Tietosuojavastaavalla on tärkeä rooli myös yrityksen turvallisuuskulttuurin luojana. Hänellä on syytä olla hyvät suhteet kaikkia tietoja käsitteleviin henkilöihin, mutta myös käsittelyn turvallisuuteen liittyviin sidosryhmiin. Tilaturvallisuus, paloturvallisuus, tietojärjestelmien turvallisuus ja toimintavarmuus ovat kaikki yhtä lailla tekijöitä, jotka vaikuttavat henkilötietojen käsittelyyn. Kukaan ei voi osata kaikkea yksin, mutta hyvällä ja rakentavalla yhteistyöllä ja kiinnostuksella omaan tehtäväänsä, voi tietosuojasta vastaava henkilö olla kullanarvoinen

apu yrittäjälle kaiken toiminnan suojaamisessa ja varmistamisessa.

Tietosuojavastaavan nimittämisestä on tehtävä ilmoitus tietosuojavaltuutetun sivuilla olevan lomakkeen kautta.

Tietosuojavastaava Hyvinvointikeidas Maijalla

Maija kävi läpi tietosuojavaltuutetun toimiston sivuilla olevat ohjeet ja erityisesti tietosuojavastaavia koskevat ohjeet. Eniten häntä mietitytti asiakkaista kerättävä tieto, joka koski terveydentilaa sekä lähetteellä tulevien fysioterapian kuntoutuspotilaiden hoitotiedot. Hän ei tiennyt, olisiko hänellä velvollisuus nimittää tietosuojavastaava, joten hän kävi erityisen huolellisesti läpi WP29:n julkaiseman liitteen asiakirjasta WP243, usein kysytyt kysymykset [35.].

Koko yritystään ajatellen Maija tulkitsi, että hänen ydintehtävänsä eivät muodostuneet henkilötietojen käsittelystä. Hänellä oli paljon asiakkaita, joiden henkilötietojen käsittely tapahtui vain laskutusta tai muuta varsinaisen ydintoiminnan tukitoimintoa varten. Lisäksi käsittely ei ollut erityisen laajamittaista, koska hän ei tuottanut työterveyspalveluita tai sopimusperusteisesti jonkin tietyn kaupungin tai kunnan palveluita. Kaikki asiakkaat saapuivat hänelle omasta tahdostaan ja valitsemalla palveluntarjoajan monien yritysten joukosta.

Valvira määrittelee fysioterapiapalvelut luvanvaraiseksi terveydenhuollon palveluksi ja Maija oli tehnyt ilmoitukset aluehallintovirastoon ja laatinut tarvittavat omavalvontasuunnitelmat sekä noudatti muutenkin lakisääteisiä velvoitteita. Aina hän ei ollut ihan varma, missä asemassa hän oli lainsäädännön näkökulmasta, mutta hän ei itse, eikä uskonut asiakkaidenkaan, mieltävän yritystään varsinaisesti lääkäripalveluiden tai terveydenhuollon toimijaksi.

Maija teki tulkinnan, että hänellä ei olisi lakisääteistä pakkoa nimetä tietosuojavastaavaa. Tietosuoja-asetus oli kuitenkin uusi asia ja tulkintaan saattoi tulla tarkennuksia myöhemmin. Siksi hän otti asian vakavasti ja päätti, että jonkun oli otettava lainsäädännön vaatimuksista huolehtiminen harteilleen. Vaihtoehtoja ei kuitenkaan ollut paljon. Roni ja Ronja opiskelivat ja tekivät työtä vain osa-aikaisesti ja Janita hoiti vain personal training -asiakkaita, eikä hänellä ollut pääsyä kaikkeen yrityksessä käsiteltävään henkilötietoon. Juha oli yksityinen yrittäjä, eikä siten ollut vaihtoehto. Vastuu jäi siis Maijalle itselle.

Maija lisäsi omat yhteystietonsa tietosuojaa koskeviin selosteisiin ja sopimuksiin. Työntekijöiden ohjeisiin kirjattiin, että kaikissa epäselvissä asioissa ja kysymyksissä oli aina otettava yhteyttä Maijaan.

Tietosuoja-asetus edellyttää, ettei tietosuojavastaava saa olla mukana päättämässä henkilötietojen käsittelyn tarkoituksista ja keinoista, mutta Maija päätti yrityksessä niistä yksin, kuten kaikesta muustakin yrityksen toimintaan liittyvistä asioista. Muita vaihtoehtoja tietosuojasta vastaavaksi ei näin ollut.

.

13. Jatkuvaa toimintaa ja laadun kehittämistä

Tietosuojalainsäädännön vaatimusten noudattaminen ei ole kertaprojekti. Ei henkilötietolainkaan noudattaminen sitä ollut, mutta lainsäädännön muuttuminen on tehnyt tietosuojan osalta merkittäviä muutoksia. Vastuu on nyt yksiselitteisesti rekisterinpitäjillä eli yhdistyksillä, yhteisöillä, yrityksillä ja kaikilla, jotka käsittelevät henkilötietoja. Merkittävää on myös osoitusvelvollisuuden suuri painoarvo. Ennen riitti, että teki oikein, nyt se on kyettävä myös osoittamaan [36.].

Lainsäädännön muutos on iso, mutta ei ennalta-arvaamaton. Pelastuslaki muuttui jo aikanaan siten, että tiukasta viranomaisvalvonnasta luovuttiin ja kiinteistöjen omistajien vastuu kasvoi pelastussuunnitelmien ja niiden valvonnan myötä. Elintarvikealalla työskentelevät ovat jo tottuneet omavalvontasuunnitelmiin ja esimerkiksi kylmäketjujen seurantaan. Terveydenhuollon omavalvontavelvoitteet kuuluvat samaan kokonaisuuteen.

Yksikään yrityksistä ei ole saanut “tietosuojan kehittämisrahoitusta”, vaikka siihen joudutaan satsaamaan nyt resursseja. Kannattaa muistaa, että tietosuojalainsäädäntöön sisäänrakennettu riskilähtöinen ajattelutapa on pienyrittäjien suoja samalla, kun velvoitteet lisääntyvät. Asetuksen johdanto-osassa on monessa kohdin otettu huomioon pienten ja mikroyritysten erilainen asema. Vapauksia velvoitteiden noudattamiseen ei ole, mutta pienissä yrityksissä on erityisen tärkeää keskittyä riskienhallintaan. Keskittymällä siihen, mikä on olennaista ja mikä muodostaa suurimman riskin, toimii asetusten vaatimusten mukaan. Vähempiarvoisiin ja ns. olemattomiin asioihin ei kannata keskittyä. Näin säästyy aikaa ja resursseja.

Tänä vuonna voi tehdä tietosuojan eteen jotain ja ensi vuonna vähän lisää. Kaikkea ei kannata yrittää tehdä heti, mutta suunnitelmallisuus ja asioiden järjestelmällinen tekeminen sekä kirjaaminen auttavat jokaista yrittäjää osoittamaan toiminnan oikean suunnan. Omien henkilötietojen käsittelytoimien riskien tunteminen on erittäin tärkeää. Kannattaa aina aloittaa siitä, missä riskit ovat suurimmat ja kirjata loput riskeihin liittyvät toimet vaikka ensi vuodelle.

Tarkistuslista

Jokaisen yrityksen toiminta on täysin erilaista. Edes samalla alalla toimivat yritykset eivät voi kopioida toistensa dokumentteja ja luottaa siihen, että kaikki on kunnossa. Pitää muistaa, että yrittäjä on myös velvollinen osoittamaan, että asiat ovat todella tehty yrityksessä.

Tähän mennessä on varmasti jo selvinnyt, että oppaan mukana ei voida antaa valmiita dokumentteja, jotka kopioimalla voisit osoittaa tietosuojalainsäädännön noudattamisen olevan kunnossa yrityksessäsi. Opas on tehty tietosuojan minimitasoa silmällä pitäen, joten pelkästään tämän oppaan mukaan toimiminen ei välttämättä riitä sinun yrityksesi kohdalla.

Oppaan liitteenä on työkaluksi tarkoitettu lomake 8, jonka avulla voi arvioida, mitä tietosuojan osa-alueita yrityksessä on huomioitu ja mihin pitäisi vielä reagoida.

Lisäksi oppaan liitteenä on lomake 9, josta löytyy listattuna asetuksen merkittävimmät velvoitteet. Lomakkeen taulukkoon voi tehdä muistiinpanoja ja päivittää sitä sen mukaan, kun tietosuojatyö yrityksessä etenee. Lainsäädäntö ja sen tulkinnat muuttuvat koko ajan, joten on myös hyvä seurata uutisointia ja tietosuojavaltuutetun sivustoa [37.]. Osa asioista voi olla turhia, mutta osa saattaa koskea juuri oman yrityksen toimintaa.

Jatkuva seuranta

Edellä olevien lomakkeiden läpikäynti ensimmäisellä kerralla jättää usein kohtia vailla vastausta. Se ei haittaa mitään, mutta pääasia on, että työ yrityksessä etenee.

Kaikkiin kysymyksiin ei ehdi saada koskaan vastausta ennen kuin asiat jo muuttuvat siten, että kysymykset on käytävä ja arvioitava taas uudelleen. Tärkeää on ymmärtää, että tietosuojalainsäädännön vaatimuksia ei voi koskaan täyttää yhdellä projektilla, jonka jälkeen asian voisi unohtaa. Sen sijaan, jos yritys kykenee osoittamaan, että tietosuojatyötä tehdään koko ajan, sitä kehitetään ja se huomioidaan arjessa ja tekemisessä, mitään valmista ja lopullista “tietosuojakansiota” ei edes tarvita.

Jos henkilötietojen käsittely yrityksessä on kevyttä tai siellä ei käsitellä erityisen suuria tietomääriä tai arkaluonteisia henkilötietoja, työ voi olla helppoa. Tähän oppaaseen kannattaa palata säännöllisesti, ja etenkin silloin, kun yrityksen toimintaan kohdistuu muutoksia. Kysymyslista kannattaa käydä läpi aina uudestaan ja päivittää kartoitukset, riskiarviot ja työntekijöiden ohjeet. Kannattaa myös vilkaista välillä viranomaisten uutisia ja nettisivuja, koska

muutoksia lainsäädäntöön ja ohjeisiin saattaa tulla ajan kuluessa.

Jos yrityksessä käsitellään henkilötietoja laajemmin ja yrityksellä on useampia työntekijöitä, voi olla tarpeen arvioida asioita useammin. Ja, ettei työstä tulisi liian raskasta, työ kannattaa pilkkoa useampaan palaan ja tehdä aina pieni osuus kerrallaan pitkin vuotta. Työn voi tehdä tätä opasta apuna käyttäen, osa kerrallaan edeten. Tarvittaessa voi myös laatia itselle vuosikellon, jonka mukaan toimii. Seuraavalta sivulta löytyy esimerkkitietosuojan vuosikellosta.

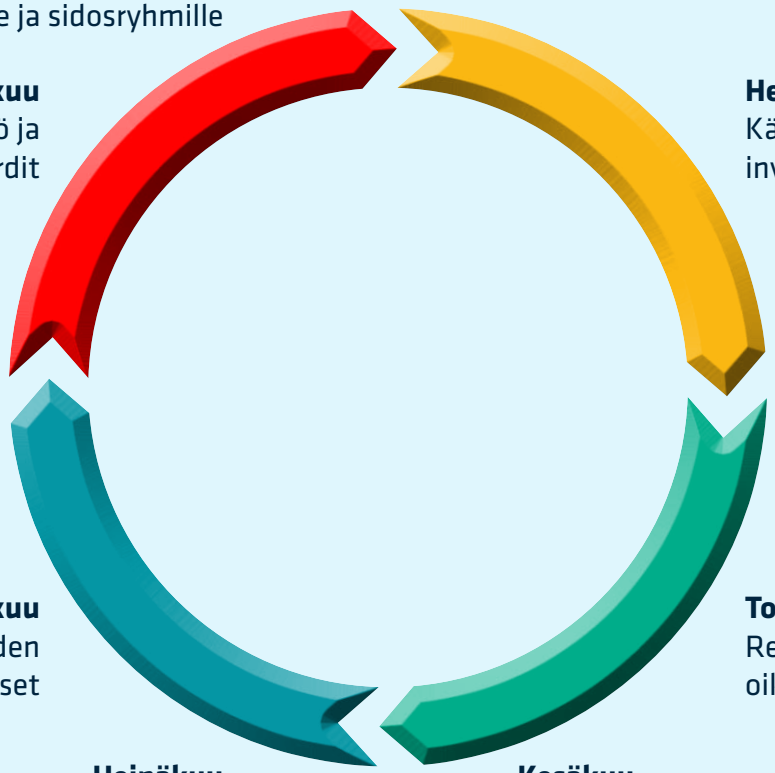
Myös näiden jatkuvien toimien tulisi hoitua yrityksen normaalin arjen mukana:

- henkilökunnan ohjeistaminen ja tukena toimiminen
- tietosuojan vaikutustenarvioinnin tarpeen arviointi ja suorittaminen tarvittaessa
- rekisteröityjen oikeuksien käyttöpyyntöihin vastaaminen
- tietosuoja-arvioinnit omasta toiminnasta
- yhteistyö valvontaviranomaisten suuntaan tarvittaessa
- oma kouluttautuminen

Tarvittaessa apuna voi käyttää ulkoisia palveluntarjoajia, mutta mitä enemmän tekee itse ja mitä parempi kokonaiskuva on oman yrityksen tarpeista, sen halvemmaksi tietosuojatyö tulee. Työn teettäminen kokonaan ulkopuolella on usein kallista, eikä tulos ole välttämättä juuri oman yrityksen näköinen. Jonkin ohjelmiston tai järjestelmän ostaminen tietosuojatarpeita varten ei myöskään ratkaise sitä ongelmaa, että itse työ on kuitenkin tehtävä.

Kannattaa luottaa yrittäjänä itseensä, koska yrittäjä tuntee aina omat asiakkaat ja työntekijät kaikkein parhaiten. Jos eteen tulee yksittäinen ylitsepääsemätön ongelma, voi sen ratkaisuun aina käyttää asiantuntijan apua.

TIETOSUOJAN VUOSIKELLO



Tammikuu
Tietosuojapolitiikka

Helmikuu
Käsittelytoimien inventointi ja rekisterit

Maaliskuu
Informointivelvoitteet ja käytännöt

Huhtikuu
Koulutussuunnittelu

Toukokuu
Rekisteröityjen oikeudet ja käyttöpyynnöt

Kesäkuu
Tietosuoja- ja tietoturva-loukkauksien hallinta

Heinäkuu
Tietosuojan mittaaminen ja tietoturvatestaukset

Elokuu
Käsittelijäsuhteiden hallinta ja sopimukset

Syyskuu
Siirrot, luovutukset ja rajat ylittävä käsittely

Lokakuu
Sisäänrakennettu ja oletusarvoinen tietosuoja

Marraskuu
Muu lainsäädäntö ja alakohtaiset standardit

Joulukuu
Vuosiraportointi johdolle ja sidosryhmille

opsec

Kiitos.

Oppaan tekstit: Jari Ala-Varvi, tietosuojavastaava, Opsec Oy

Oppaan ulkoasu: Annukka Talvitie, markkinointi ja viestintä, Opsec Oy

Suomen Yrittäjäopisto

Euroopan maaseudun kehittämisen maatalousrahasto: Eurooppa investoi maaseutualueisiin

MAASEUTU 2020

Elinkeino-, liikenne- ja ympäristökeskus