Tietosuojaopas asiakastapahtumia varten yritykselle

Jasu Pyykkö

Haaga-Helia ammattikorkeakoulu
Liiketalouden koulutusohjelma
Opinnäytetyö
2025

Tiivistelmä

Tekijä(t)
Jasu Pyykkö

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Tietosuojaopas asiakastapahtumia varten yritykselle

Sivu- ja liitesivumäärä
66 + 40

Yleinen tietosuoja-asetus on henkilötietojen käsittelyä koskeva laki, joka tuli voimaan kaikissa EU-maissa keväällä 2018. Yleinen tietosuoja-asetus on ollut jo useamman vuoden voimassa, mutta silti uutisista saadaan edelleen seurata kuinka eri organisaatiot tyrivät kerta toisensa jälkeen tietosuoja-asioidensa kanssa. Tietosuojan kanssa epäonnistuminen on harmillista, koska sen pettäessä ihmisten luottamus organisaatiota kohtaan voi murentua pahimmassa tapauksessa jopa peruuttamattomasti.

Tämä opinnäytetyö on toteutettu toiminnallisena opinnäytetyönä, ja sen tuotoksena tehtiin tietosuojaopas asiakastapahtumia varten yritykselle. Tietosuojaopas tehtiin toimeksiantona Planmeca Oy:lle vastaamaan yrityksen tietosuoja-asiantuntijoiden tarpeita. Tietosuojaopasta on tarkoitus hyödyntää yrityksen asiakastapahtumien tietosuojallisessa järjestämisessä. Lisäksi opas vastaa yleisen tietosuoja-asetuksen osoitusvelvollisuuden vaatimuksiin ohjeistaa yrityksen työntekijöitä henkilötietojen käsittelyn eri vaiheissa erilaisin keinoin. Tietosuojaopas on tehty konstruktiivisella kehittämistyön menetelmällä ja sen aikaansaamiseksi on hyödynnetty tietosuojavaltuutetun toimiston verkkosivuja, ammattikirjallisuutta sekä Planmeca Oy:n tietosuoja-asiantuntijoita.

Opinnäytetyön tietoperusta on jaettu kolmeen osaan. Ensimmäisessä osiossa käsitellään henkilötietojen käsittelyä koskevia perusperiaatteita, koska jokaisen organisaation työntekijän on hyvä ymmärtää esimerkiksi, miten rekisteröidyn oikeudet tulee huomioida tai millä perustein rekisteröidyltä voi kerätä tietoja. Toisessa osiossa keskitytään tarkastelemaan asiakastapahtumaa ja sen markkinointia koskevia tietosuojasäännöksiä. Osiossa käsitellään muu muassa suoramarkkinointia koskevia sääntöjä, tapahtuman tietosuojarooleja, arvontojen henkilötietojen keräystä ja tapahtuman aikana tapahtuvaa valo- ja videokuvausta. Kolmannessa osiossa käsitellään lyhyesti, millainen rakenne ja visuaalinen olemus on hyvällä oppaalla.

Opinnäytetyötä ja sen tuotosta, eli tietosuojaopasta aloitettiin tekemään marraskuussa 2024 ja kummatkin saatiin valmiiksi maaliskuussa 2025. Tietosuojaopas toteutettiin graafisen suunnittelun verkkotyökalu Canvalla. Tietosuojaoppaan alussa on tietosuojasanastoa, jossa on selitetty mitä hankalat tietosuojaan liittyvät sanat tarkoittavat. Sanaston jälkeen tulee oppaan teoriaosuus, jonka rakenne noudattelee opinnäytetyön tietoperustan rakennetta. Tietosuojaoppaan lopussa sen sisältö on tiivistetty muistilistaan, jossa kerrataan mitä asioita henkilötietojen käsittelyssä tulee huomioida asiakastapahtumia järjestettäessä.

Tietosuojasta huolehtiminen on organisaation jokaisen työntekijän vastuulla. Huolehtimalla asiakastapahtumaan osallistuvien henkilöiden tietosuojasta, huolehditaan samalla myös asiakkaiden luottamuksen säilymisestä organisaatiota kohtaan.

Asiasanat
Tietosuoja, henkilötietojen käsittely, tietosuojaopas, asiakastapahtuma

Sisällys

1 Johdanto

Yleinen tietosuoja-asetus, joka tunnetaan myös nimellä GDPR (General Data Protection Regulation), on henkilötietojen käsittelyä koskeva laki, joka tuli voimaan kaikissa EU-maissa keväällä 2018. Sen tarkoituksena on parantaa henkilötietojen suojaa, vastata digitalisaation haasteisiin ja yhdenmukaistaa tietosuojasääntelyä EU-maissa. Laissa määritellään muun muassa, miten henkilötietoja on käsiteltävä organisaatioissa läpinäkyvästi, lainmukaisesti, luottamuksellisesti ja turvallisesti tietosuojaperiaatteiden mukaisesti. (Tietosuojavaltuutetun toimisto 2024a.) Yleistä tietosuoja-asetusta täydentää Suomessa lisäksi muun muassa kansallinen tietosuojalaki (Tietosuojalaki 5.12.2018/1050).

Tietosuojan toteutuminen on tärkeää yrityksille ja organisaatioille, koska sen pettäessä asiakkaiden luottamus voi murentua peruuttamattomasti yritystä tai organisaatiota kohtaan. Viime vuosina tietoturvaloukkaukset ja tietosuojaan liittyvät kysymykset ovatkin aiheuttaneet yrityksille paljon päänvaivaa ja saaneet ihmiset entistä kiinnostuneemmaksi siitä, miten heidän henkilötiedoistansa huolehditaan, tai ei huolehdita. (Aalto-Setälä & Viitaila 2020, 4.) Esimerkiksi Verkkokauppa.com määrättiin maksamaan vuoden 2024 keväällä lähes miljoonan euron seuraamusmaksu asiakastietojen säilytysajan määrittelemättä jättämisestä (Tietosuojavaltuutetun toimisto 2024b). Aalto-Setälä ja Viitaila (2020,4) väittävätkin, että tulevaisuudessa menestyjiä ovat ne yritykset, jotka eivät kärsi tietosuojaan liittyvistä mainehaitoista ja onnistuvat saavuttamaan tunnettuutta tietosuojan kannalta turvallisina yrityksinä.

Tämän toiminnallisen opinnäytetyön aiheena on tehdä henkilötietojen käsittelyä varten opas Planmeca Oy:n asiakastapahtumien järjestämisiä varten. Planmeca Oy on suomalainen perheyritys, joka on yksi maailman johtavista terveysteknologian laitevalmistajista. Opas on siksi tarpeellinen, koska asiakastapahtumissa saatetaan joutua käsittelemään hyvinkin paljon asiakkaiden henkilötietoja, kuten esmerkiksi ruokavalioihin liittyviä tietoja, jotka kuuluvat arkaluontoisiin henkilötietoryhmiin. Planmeca Oy:n tapahtumissa yleensä myös kuvataan vieraita, ja heistä saatetaan julkaista kuvamateriaalia sosiaalisessa mediassa.

Oppaan tekeminen liittyy yleisen tietosuoja-asetuksen säännöksiin osoitusvelvollisuudesta. Osoitusvelvollisuus tarkoittaa sitä, että organisaation on pystyttävä osoittamaan, että se pyrkii toiminnassaan suojaamaan erilaisin toimenpitein henkilötietojen, kuten ihmisten kuvien, sähköpostiosoitteiden tai nimien oikeanlaisen käsittelyn (Tietosuojavaltuutetun toimisto 2024c).

1.1 Tavoitteet, rajaus ja menetelmät

Opinnäytetyönä syntyvän tietosuojaoppaan tavoitteena on luoda Planmeca Oy:n markkinointi- ja viestintäosastolle ja muille asiakastapahtumia järjestäville toimihenkilöille mahdollisimman selkeä ja helppolukuinen tietopaketti asiakastapahtumien järjestämisestä tietosuojaan liittyen. Opinnäytetyön tarkoituksena ei siis ole esitellä yleistä tietosuoja-asetusta ja muita tietosuojaan liittyviä lakeja yksityiskohtaisesti, vaan löytää yleisiä ohjeita ja käytänteitä onnistuneen tapahtuman järjestämiseksi henkilötietojen käsittelyn näkökulmasta. Opinnäytetyö ja sen tuotoksena syntyvä opas ei siis tule vastaamaan täsmällisesti kysymyksiin tietoturvasta, yksityisyyden suojasta tai esimerkiksi siitä kenelle tapahtumasta otetun valokuvan tekijänoikeudet kuuluvat tai millaisella kovalevyllä henkilötietoja olisi hyvä säilyttää. Opinnäytetyö pyrkii antamaan vastauksia tietosuojan perusasioissa sekä yleisissä tapahtuman järjestämiseen liittyvissä tietosuojakysymyksissä ja siitä, kuinka niihin tulisi kiinnittää huomiota tapahtuman eri vaiheissa.

Tämän toiminnallisen opinnäytetyön kehittämistyön menetelmänä toimii konstruktiivinen tutkimus. Opinnäytetyön tekemisessä käytetään tietosuojaan liittyvää ammattikirjallisuutta, viranomaissivustoja ja muita lähteitä. Osana opinnäytetyötä ovat palaverit ja ryhmäkeskustelut Planmeca Oy:n tietosuojavastaavan ja tietosuoja-asiantuntijoiden kanssa. Tällä tavoin opinnäytetyönä syntyvä opas saadaan paremmin vastaamaan Planmeca Oy:n tietosuoja-asiantuntijoiden tarpeita.

Opinnäytetyön tietoperustassa tullaan lyhyesti käsittelemään myös omana kokonaisuutena asioita, jotka olisi hyvä ottaa huomioon visuaalista opasta tehdessä. Opinnäytetyön painopiste ei kuitenkaan ole vastata kysymykseen ”Millainen on hyvä opas visuaalisesti?”, joten siksi aihetta käsitellään vain lyhyesti. Oppaan tekemisessä hyödynnetään Canva -sovellusta, joka on graafisen suunnittelun verkkotyökalu. Asiakastapahtumien järjestämisiä varten tehdyn tietosuojaoppaan onnistumisen mittarina voidaan pitää sitä, kokevatko Planmeca Oy:n tietosuojavastaava ja muut työntekijät oppaan hyödyllisenä vai eivät.

Planmeca Oy on sitoutunut vastuullisuuteen, kestävään kehitykseen ja ihmisten hyvinvointiin. Siksi opinnäytetyönä syntyvä opas tukee hyvin Planmeca Oy:n tavoitteita toimia vastuullisena organisaationa. Kun tietosuojaan liittyvät asiat hoidetaan Planmeca Oy:llä mahdollisimman hyvin, niin yrityksellä on mahdollisuus myös suorittaa ISO 27701 sertifiointi. Sertifiointi kertoisi asiakkaille, että Planmeca Oy välittää työntekijöidensä, asiakkaidensa ja vieraidensa henkilötietojen turvallisesta käsittelystä.

1.2 Keskeiset tietosuojaan liittyvät käsitteet

Tietosuojaan kuuluu paljon erilaista termistöä, joista osa voi olla hankala ymmärtää. Tämän vuoksi seuraavaksi esitellään opinnäytetyössä esiintyviä tietosuojaan liittyviä käsitteitä. Käsitteet on esitelty aakkosjärjestyksessä.

Alikäsittelijäksi kutsutaan tahoa, joka käsittelee henkilötietoja henkilötietojen käsittelijän puolesta. Alikäsittelijä voi olla esimerkiksi yritys, viranomainen, yhdistys tai muu toimija, joka käsittelee henkilötietoja henkilötietojen käsittelijän ohjeistamana. Jotta alikäsittelijä voidaan hyödyntää, pitää rekisterinpitäjän tai yhteisrekisterinpitäjän antaa tähän kirjallinen hyväksyntä. (European Data Protection Board 2024.)

Anonymisoinnilla tarkoitetaan henkilötietojen käsittelyä pysyvästi siten, että niitä ei pysty enää yhdistämään kehenkään tiettyyn henkilöön. Anonymisoinnin jälkeen tietoja ei enää katsota henkilötiedoiksi, joten niiden käsittelyä ei enää rajoita tietosuojasäännökset. (Keller 2023, 154.)

Erityisiin henkilötietoryhmiin kuuluvat arkaluontoiset henkilötiedot, joiden käsittely yrityksissä ja muissa organisaatioissa on alustavasti kiellettyä. Erityisiin henkilötietoryhmiin kuuluvat tiedot ihmisen rodusta tai etnisestä alkuperästä, sukupuolisesta suuntautumisesta, poliittisista mielipiteistä, uskonnollisista tai filosofisista vakaumuksista, ammattiliittoon kuulumisista sekä geneettiset, biometriset tai terveydelliset tiedot. Erityisiä henkilötietoja saa käsitellä vain silloin kun se on mahdollista EU:n yleisen tietosuoja-asetuksen tai kansallisen lainsäädännön puitteissa. Esimerkiksi sairaaloissa tai vakuutusyhtiöissä erityisiä henkilötietoryhmiä on säilytettävä hyvin varovaisesti. (Andreasson, Oravala & Toivonen 2023, 44.)

Evästeet ovat tietojoukkoja, joilla digitaalisen palvelujen tarjoaja seuraa selaimen käyttäjän toimintaa esimerkiksi linkkien käytöstä ja muista valinnoista. Evästeitä hyödynnetään muun muassa verkkosivustojen suoramarkkinoinnissa, kävijämäärien tilastoimisessa sekä palvelujen kehittämistarpeita pohdittaessa. Evästeitä ja niihin liittyvää seurantateknologiaa ei saisi käyttää sivustolle tultaessa, vaan siihen tulisi kysyä käyttäjältä lupa. Tietoja saa kerätä vain silloin kun siihen on suostuttu ja ne ovat välttämättömiä digitaalisen palvelun, kuten esimerkiksi verkkokaupan ostoskorin toimimiseksi. (Voutilainen 2023, 233–234.)

Henkilötietoja ovat kaikki ne tiedot, joiden perusteella henkilö voidaan tunnistaa joko suoraan tai välillisesti yhdistämällä henkilöä kuvaavan tieto johonkin toiseen tietoon. Henkilötietoja ovat esimerkiksi nimi, asuinosoite, henkilötunnus, puhelinnumero, sähköpostiosoite, ihmisen valokuva, ihmisen ääni, IP-osoite, auton rekisterinumero, passin numero, kulttuurinen profiili ja opiskelijatiedot. Henkilötietoja eivät ole esimerkiksi yrityksen rekisteritunnus, organisaation yleinen sähköpostiosoite tai anonymisoidut tiedot. (Andreasson ym. 2023, 42–43.) Henkilötietoja voidaan säilyttää

esimerkiksi sähköisissä tiedostoissa, paperilla tai ääni- tai kuvatallenteella (Tietosuojavaltuutetun toimisto 2024d).

Henkilötietojen käsittelijä on ulkopuolinen henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Ulkopuolinen henkilö voi olla esimerkiksi alihankkija tai yhteistyökumppani, jolle rekisterinpitäjä on ulkoistanut tietojen käsittelyä, kuten säilyttämistä. Henkilötietojen käsittelijä toimii rekisterinpitäjän antamien ohjeiden mukaan, eikä hän saa itsenäisesti päättää tietojen keräämisestä tai käytöstä. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 22.)

Henkilötietojen käsittelyllä tarkoitetaan lähes kaikenlaisia toimintoja, joissa on mukana henkilötietoja. Käsittely voi olla esimerkiksi tietojen keräämistä, säilyttämistä, muokkaamista, luovuttamista, yhdistämistä, rajoittamista, poistamista tai tuhoamista. (Hanninen ym. 2017, 20–21.)

Kolmannella osapuolella tarkoitetaan yleisen tietosuoja-asetuksen 4 artiklan 10 kohdan mukaan jotain muuta henkilöä kuin rekisterinpitäjää, henkilötietojen käsittelijää, rekisteröityä tai muuta henkilöä, joka käsittelee henkilötietoja rekisterinpitäjän vastuun alaisena ja jolla on oikeus siihen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)).

Profiloinnilla tarkoitetaan toimintaa, jossa rekisterinpitäjä tallentaa ja analysoi automaattisen päätöksenteon avulla rekisteröidystä tietoja, joiden perusteella esimerkiksi arvioidaan tai ennustetaan hänen kykyjään tai mielenkiinnon kohteitaan. Profiloinnissa luotonantaja voi esimerkiksi käyttää päätöksentekonsa tukena asiakasdatasta rakennettua algoritmia. Rekisteröidylle tulee ilmoittaa profiloinnista, jos sitä hyödynnetään rekisteröidyn henkilötietojen käsittelyssä ja analysoinnissa. (Korpisaari, Pitkänen & Warma-Lehtinen 2022, 71.)

Pseudonymisoinnissa henkilötietoja muutetaan siten, että niitä ei pysty täsmällisesti yhdistämään kehenkään henkilöön. Pseudonymisointi eroaa anonymisoinnista siten, että muutetut tiedot voidaan halutessa palauttaa alkuperäiseen muotoonsa ja yhdistää ne takaisin henkilöön kenen tietoja muutettiin. Tietojen muuttaminen ja yhdistäminen voidaan toteuttaa esimerkiksi yksilöivän koodin avulla. Pseudonymisoituihin tietoihin sovelletaan tietosuojasäännöksiä, koska näiden tietojen katsotaan yhä olevan henkilötietoja yksilöivän koodinsa ja palautettavuutensa takia. (Keller 2023, 154.)

Rajat ylittävällä käsittelyllä tarkoitetaan yleisen tietosuoja-asetuksen 4 artiklan 23 kohdan mukaan henkilötietojen käsittelyä, joka tapahtuu useammassa kuin yhdessä valtiossa. Rajat ylittävää käsittelyä on esimerkiksi se, kun rekisterinpitäjä tai henkilötietojen käsittelijä käsittelee tietoja useammassa kuin yhdessä toimipaikassa vähintään kahdessa eri valtiossa. Rajat ylittäväksi

käsittelyksi katsotaan myös se, kun rekisterinpitäjän tai henkilötietojen käsittelijän käsittely vaikuttaa useammassa kuin yhdessä valtiossa oleviin rekisteröityihin, vaikka käsittely tapahtuisikin yhdessä toimipaikassa yhden valtion rajojen sisällä. (yleinen tietosuoja-asetus.)

Rekisterillä tarkoitetaan yleisen tietosuoja-asetuksen mukaan mitä tahansa henkilötietoja sisältävää tietojoukkoa, mistä tiedot ovat saatavilla tietyin perustein. Rekisteriä voidaan ylläpitää esimerkiksi tietoteknisesti tietokoneella tai perinteisesti paperilla arkistoissa. Henkilörekistereitä voivat olla esimerkiksi jäsen-, käyttäjä- ja asiakasrekisterit sekä osallistujaluettelot. (Korpisaari ym. 2022, 73.)

Rekisterinpitäjä voi olla yritys, yhdistys, sairaala, koulu, verkkokauppa, yksityishenkilö, viranomainen tai muu taho, joka käsittelee henkilötietoja. Rekisterinpitäjän velvollisuuksiin kuuluu suunnitella ja valvoa henkilötietojen käsittelyä sekä määritellä miksi ja miten henkilötietoja kerätään ja säilytetään. Rekisterinpitäjä on aina lopullisessa vastuussa henkilötietojen käsittelystä, mutta rekisterinpitäjä voi käyttää toimessaan apuna ulkopuolista henkilötietojen käsittelijää esimerkiksi tietojen teknistä säilyttämistä varten. Rekisterinpitäjän tehtäviin kuuluu myös tietosuojaselosteen tekeminen. (Järvinen 2022, 136.)

Rekisteröidyksi kutsutaan henkilöä, kenen henkilötietoja rekisterinpitäjä käsittelee. Rekisteröidyllä on yleisen tietosuoja-asetuksen mukaan monia oikeuksia, kuten oikeus tarkastaa mitä tietoja rekisterinpitäjä on kerännyt hänestä. (Andreasson ym. 2023, 266.)

Suostumuksella tarkoitetaan rekisteröidyn hyväksyntää henkilötietojensa käsittelylle. Suostumuksen tulee olla aidosti vapaaehtoinen ja sen antamisesta on myös pystyttävä kieltäytymään. Suostumusta tulee kysyä henkilötietoja kerättäessä, jotta rekisteröidyllä on mahdollisuus harkita mitä tietoja hän on valmis jakamaan. (Tietosuojavaltuutetun toimisto 2024e.)

Tietojenkäsittelysopimus tai henkilötietojen käsittelysopimus (data processing agreement, DPA) tehdään silloin kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta tai lukuun. Sopimuksessa olisi hyvä kuvata muun muassa henkilötietojen käsittelyn kesto, käsittelyn luonne ja tarkoitus, mitä henkilötietoja käsitellään sekä rekisterinpitäjän velvollisuudet ja oikeudet. Henkilötietojen käsittelijä toimii aina rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Rekisterinpitäjä voi antaa nämä ohjeet tietojenkäsittelysopimuksessa. (Hanninen ym. 2017, 82–84.)

Tietosuojaseloste on kirjallinen kuvaus siitä, kuinka rekisterinpitäjä käsittelee henkilötietoja. Tietosuojaselosteen tulisi vastata muun muassa esimerkiksi siihen, mihin tarkoituksiin organisaatio käyttää pyytämiään tietoja, kuinka kauan rekisteröidyn tietoja säilytetään ja minkälaiset oikeudet rekisteröidyllä on. (Andreasson ym. 2023, 114–115.)

Tietosuojavaltuutettu ja tietosuojavaltuutetun toimisto toimii kansallisena tietosuojaviranomaisena Suomessa. Tietosuojaviranomaisella on oikeus muun muassa tutkia rekisterinpitäjän tai henkilötietojen käsittelijän henkilötietojen käsittelyä, antaa ohjeita ja neuvoja tietojenkäsittelystä, pyrkiä toimillaan korjaamaan puutteellisia henkilötietojen käsittelyyn liittyviä käytänteitä esimerkiksi antamalla varoituksen, määräyksen tai huomautuksen rekisterinpitäjälle tai henkilötietojen käsittelijälle. Tietosuojaviranomainen voi myös määrätä hallinnollisia seuraamusmaksuja, eli sakkoja. (Andreasson & Ylipartanen 2022, 228–237.)

Tietosuojavastaava on organisaation, kuten esimerkiksi kunnan, yrityksen tai muun organisaation sisäinen asiantuntija tietosuojaan liittyvissä asioissa. Tietosuojavastaava huolehtii siitä, että organisaation koko henkilöstö johtoa myöten noudattaa tietosuojasäännöksiä, ja tarvittaessa myös ohjeistaa heitä tietosuojaan liittyvissä ongelmatilanteissa. Jos organisaatiossa käsitellään arkaluontoisia henkilötietoja laajamittaisesti tai seurataan ihmisten toimintaa, on tietosuojavastaava nimitettävä. Rekisteröidyillä on oikeus olla tietosuojavastaavaan yhteydessä kaikissa heidän henkilötietojensa käsittelyihin liittyvissä asioissa. (Andreasson ym. 2023, 267.)

Tietoturva on yksi niistä menetelmistä, jolla organisaatioissa varmistetaan tietosuojan toteutuminen. Tietoturvan avulla suojataan teknisesti tietoaineistot ja tietojärjestelmät, joissa esimerkiksi rekisteröityjen tietoja säilytetään. Asianmukaisella tietoturvalla varmistetaan tietojen saatavuus, eheys, käytettävyys, luottamuksellisuus ja rekisteröidyn oikeuksien toteutuminen. (Andreasson ym. 2023, 267–268.)

Tietoturvaloukkauksella tarkoitetaan tilannetta, jossa henkilötietoja häviää, tiedot muuttuvat tai tietoja päätyy henkilöille, joilla ei pitäisi olla oikeutta niihin. Tietoturvaloukkaus voi liittyä tietomurtoihin tai hakkerointiin, mutta myös esimerkiksi muistitikun, puhelimen tai salasanojen häviäminen ovat tietoturvaloukkauksia. (Andreasson ym. 2023, 108.)

Yhteisrekisterinpitäjäksi kutsutaan rekisterinpitäjiä, jotka määrittelevät keskenään henkilötietojen käsittelyn tarkoituksen ja keinot. Yhteisrekisterinpitäjiä tulee olla vähintään kaksi, mutta niitä voi olla myös useampia. Yhteisrekisterinpitäjien täytyy myös sopia keskenään kunkin yhteisrekisterinpitäjän vastuut ja toimet henkilötietojen suojaamiseksi. (European Data Protection Board 2024)

Vaikutustenarviointi (data protection impact assessment, DPIA) on menettely, jonka tarkoituksena on tutkia ja tunnistaa tietosuojan toteutumiseen liittyviä riskejä ja uhkia suhteessa hyötyihin ja rekisteröidyn oikeuksiin. Vaikutustenarvioinnin avulla voidaan pohtia mitä toimenpiteitä ja päätöksiä kannattaa tehdä organisaatiossa, jotta rekisteröityjen henkilötietojen käsittely olisi mahdollisimman turvallista ja tietosuoja-asetusten mukaisia. (Hanninen ym. 2017, 115.)

2 Henkilötietojen käsittelyä koskevat perusperiaatteet

Puhuttaessa henkilötietojen käsittelystä esiin nousevat yleensä käsitteet tietosuoja, yksityisyys ja tietoturva. Nämä kaikki sanat liittyvät toisiinsa, mutta eivät tarkoita samaa asiaa. Siksi opinnäytetyön tietoperustan aluksi on hyvä määritellä selkeyden vuoksi, miten kyseiset käsitteet eroavat toisistaan.

Yksityisyys on sitä, että ihminen saa itse päättää mitä tietoja hän jakaa itsestään ja kenelle esimerkiksi sosiaalisessa mediassa. Tietosuojalla tarkoitetaan sääntöjä, jotka määrittelevät miten henkilötietoja kuuluu käsitellä. Esimerkiksi kuluttajalle saa tehdä sähköistä suoramarkkinointia vain silloin kun hän on itse antanut siihen luvan. Tietosuojaa ja sen toteutumista valvotaan viranomaisten toimesta. Yksityisyydestään ihminen huolehtii itse ja tekee omantuntonsa mukaisia päätöksiä siitä, mitä tietoja hän haluaa kertoa itsestään muille. Tietoturvalla tarkoitetaan kaikkia niitä teknisiä toimenpiteitä, joilla turvallinen henkilötietojen käsittely, kuten tietojen säilyttäminen onnistuu. Esimerkiksi erilaiset virustorjuntaohjelmat suojaavat yrityksiä ja kuluttajia identiteettivarkauksilta. Tämän vuoksi tietoturvalla on valtava rooli tietosuojan ja yksityisyyden toteutumisessa. (Keller 2023, 48–58.)

Yleistä tietosuoja-asetusta ei ole tehty estämään henkilötietojen käsittelyä, vaan mahdollistamaan henkilötietojen asianmukainen käsittely. On tärkeää, että on olemassa sääntöjä siihen ketkä saa käsitellä henkilötietoja, mitä tarkoituksia varten tietoja saa käsitellä ja kuinka kauan tietoja on mahdollista säilyttää. Yleisessä tietosuoja-asetuksessa organisaatioille on asetettu myös vaatimuksia tietoturvan tason suhteen henkilötietojen suojaamiseksi. (Keller 2023, 51–54.)

EU:n yleistä tietosuoja-asetusta ei kuitenkaan sovelleta niissä tapauksissa, kun rekisteröity on kuollut tai on oikeushenkilö, eli esimerkiksi yritys tai julkisoikeudellinen taho. Yleistä tietosuoja-asetusta ei sovelleta myöskään silloin kun henkilötietoja käsittelee yksityishenkilö omia henkilökohtaisia tarkoituksia varten. Esimerkiksi yksityishenkilöön ei sovelleta tietosuoja-asetusta, jos hän on tallentanut omaan kännykkäänsä yhteystietoja yksityistä käyttöä varten. (Andreasson ym. 2023, 48–49.)

Suomessa on olemassa oma kansallinen tietosuojalaki (1050/2018), joka toimii yleisen tietosuoja-asetuksen rinnalla. Tietosuojalain tarkoituksena on täydentää ja selkeyttää yleistä tietosuoja-asetusta. Tietosuojalaissa säädetään muun muassa tietosuojavaltuutetun nimittämisestä, tietosuojavaltuutetun toimiston toimivaltuuksista, henkilötunnusten käsittelystä, rajoituksista rekisteröityjen oikeuksiin sekä tilanteista, joissa yleinen etu on oikeusperuste henkilötietojen käsittelylle. Suomessa muita henkilötietojen käsittelyyn kantaa ottavia lakeja ovat muun muassa laki yksityisyyden

suojasta työelämässä (759/2004) sekä laki sähköisen viestinnän palveluista (917/2014). (Andreasson ym. 2023, 49–50.)

2.1 Tietosuojaperiaatteet

Yleisessä tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyn periaatteista, joiden tarkoituksena on ohjata organisaatioiden tietojen käsittelyä. Tietosuoja-periaatteet siis neuvovat mitä tietoja on hyväksyttyä käsitellä ja miten. Tietosuojaperiaatteita ovat käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus, käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys sekä rekisterinpitäjän osoitusvelvollisuus. (Hanninen ym. 2017, 47–48.)

2.1.1 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus tarkoittaa sitä, että rekisterinpitäjän on kerättävä henkilötietoja vain tiettyä ennalta määriteltyä lainmukaista asiaa tai tehtävää varten. Rekisterinpitäjä ei saa käyttää kerättyjä henkilötietoja myöhemmin muuhun tarkoitukseen kuin mitä varten tiedot oli alun perin kerätty. Henkilötietoja voidaan kerätä esimerkiksi suoramarkkinointia, asiakassuhteiden hoitoa ja työntekijöiden valintaa varten. Henkilötietoja ei saa kerätä tai käsitellä sellaisissa tapauksissa, kun sille ei ole mitään perusteita. (Hanninen ym. 2017, 49.)

2.1.2 Tietojen minimointi

Tietojen minimointi tarkoittaa sitä, että rekisteröidyltä saa kerätä ja käsitellä käyttötarkoituksen kannalta vain tarpeellisia henkilötietoja. Eli toisin sanoen rekisteröidyltä kerättävät ja käsiteltävät henkilötiedot tulee pitää minimissään. Tämä edellyttää rekisterinpitäjältä sitä, että hän määrittelee henkilötietojen käsittelyn tarkoituksen, huolehtii säilytettävien henkilötietojen oikeellisuudesta päivittämällä tietoja tarpeen tullen sekä poistamalla tarpeettomat ja virheelliset tiedot. Tietojen säilytysaika tulee pitää myös niin lyhyenä kuin mahdollista, eikä tietoja saa säilyttää varmuuden vuoksi myöhempää käyttöä varten, jos sille ei ole esimerkiksi lakiin perustuvaa velvoitetta tai muuta syytä. (Korpisaari ym. 2022, 29.) Vaikka rekisteröity olisi antanut esimerkiksi suostumuksensa henkilötietojensa säilyttämiseen, se ei kuitenkaan oikeuta säilyttämään tietoja kauempaa kuin on välttämätöntä (Hanninen ym. 2017, 50).

2.1.3 Tietojen täsmällisyys

Tietojen täsmällisyys tarkoittaa sitä, että käsiteltävien henkilötietojen tulee olla virheettömiä ja ajantasaisia. Rekisterinpitäjä on vastuussa tietojen oikeellisuudesta ja väärät sekä puutteelliset tiedot on korjattava tai poistettava aina niin pian kuin vain mahdollista. Esimerkiksi epätarkat ja vanhat

tiedot ihmisten terveydentilasta ja hoitohistoriasta voivat aiheuttaa terveydelle vaarallisia tilanteita sairaanhoidossa. Väärät tiedot voivat siis merkittävällä tavalla vaarantaa rekisteröidyn oikeuksia, joten siksi rekisterinpitäjän täytyy huolehtia tietojen säännöllisestä tarkastamisesta. Rekisteröidyllä on myös oikeus tarkastella, korjata ja pyytää tietojensa poistamista rekisterinpitäjältä. Rekisterinpitäjän täytyy myös ilmoittaa kaikista henkilötietojen muutoksista niille tahoille, keille rekisteröidyn henkilötietoja on luovutettu. (Tietosuojavaltuutetun toimisto 2024f.)

2.1.4 Tietojen säilytyksen rajoittaminen

Tietojen säilytyksen rajoittamisella tarkoitetaan sitä, että henkilötietoja tulee säilyttää organisaatiossa vain niin kauan kuin henkilötiedot ovat tarpeellisia. Rekisterinpitäjän tulee esimerkiksi asiakassuhteen loppuessa päättää, ovatko asiakkaan tiedot organisaatiolle vielä tarpeellisia, vai olisiko ne aiheellista poistaa. Tarpeellisia syitä henkilötietojen säilyttämiselle voi olla esimerkiksi laskutus, perintä, oikeudelliset perusteet, reklamaatio tai takuu. Mikäli myytävästä tuotteesta halutaan tilastollisista syistä säilyttää esimerkiksi ostohistoriatietoja, tulee näistä tiedoista anonymisoida tuotteen hankkineiden henkilötiedot siten, etteivät rekisteröidyt ole tiedoista enää yksilöitävissä. (Hanninen ym. 2017, 50.) Rekisterinpitäjän tulee myös pystyä perustelemaan tarpeen tullen henkilötietojen säilyttämisen ajat sekä myös dokumentoitava ne (Tietosuojavaltuutetun toimisto 2024g).

2.1.5 Tietojen eheys ja luottamuksellisuus

Tietojen eheys ja luottamuksellisuus tarkoittaa sitä, että henkilötietoja käsitellään turvallisesti ja siten, että ulkopuolisilla ei ole pääsyä tietoihin. Rekisterinpitäjän tulee huolehtia turvallisuuden takaamiseksi tarpeellisten suojatoimien, kuten riskien, tietosuoja- ja tietoturvaohjeistuksen riittävyyden ja henkilötietojen teknisen suojauksen arvioimisesta. Rekisteröityjen henkilötiedot ovat tärkeä turvata tietoturvaloukkauksilta, koska pahimmillaan ne voivat johtaa esimerkiksi identiteettivarkauksiin tai petoksiin. Rekisterinpitäjän tulisi tarvittaessa myös huolehtia siitä, että tietoturvaloukkauksen kohteena olleet henkilötiedot pystyttäisiin palauttamaan. (Tietosuojavaltuutetun toimisto 2024h.)

2.1.6 Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja tulee käsitellä lainmukaisesti. Tämä tarkoittaa sitä, että henkilötietojen käsittely pitää tehdä yleistä tietosuoja-asetusta ja muita henkilötietojen käsittelyä koskevia kansallisia lakeja kunnioittaen. Henkilötietojen käsittelyn on myös pohjauduttava lailliseen perusteeseen, kuten oikeutettuun etuun. Läpinäkyvyydellä tarkoitetaan sitä, että rekisteröidylle tulisi kertoa ymmärrettävästi tietojen keruun yhteydessä, miten ja mitä varten hänen henkilötietojaan kerätään, ja kuinka niitä tullaan käsittelemään. Lisäksi läpinäkyvyys edellyttää, että rekisteröidylle kerrotaan hänen oikeuksistaan. (Hanninen ym. 2017, 48.) Kohtuullisuudella tarkoitetaan sitä, että rekisterinpitäjä ottaa

henkilötietojen käsittelyssä huomioon rekisteröidyn edun ja käyttää tietoja vain siihen tarkoitukseen mitä varten rekisteröity on luovuttanut tietonsa (Korpisaari ym. 2022, 29).

2.1.7 Rekisterinpitäjän osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän on pystyttävä näyttämään, että tietosuojalainsäädäntöä noudatetaan kaikissa henkilötietojen käsittelyn vaiheissa organisaatiossa. Rekisterinpitäjän tulee siis dokumentoida henkilötietojen käsittelyyn liittyvät tavat, jotta se voi jälkikäteen osoittaa noudattaneensa tietosuojaperiaatteita esimerkiksi tietoturvaloukkauksen sattuessa. Dokumentaation olisi hyvä sisältää muun muassa kuvaus tietojen teknisestä suojauksesta, kuten virustorjunnasta tai fyysisten tilojen kulkuoikeuksista, organisaation salasanapolitiikasta, henkilöstön tietosuojakoulutuksista, riski- ja vaikutustenarvioinneista sekä miten esimerkiksi rekisteröityjen oikeudet huomioidaan tietoturvaloukkauksen sattuessa organisaatiossa. Dokumentaatiota on aina päivitettävä, kun esimerkiksi organisaation henkilötietojen käsittelyyn liittyviin järjestelmiin tulee muutoksia, tai organisaation henkilötietojen käsittelyä uudistetaan. (Hanninen ym. 2017, 51–53.)

2.2 Henkilötietojen käsittelyn peruste

Henkilötietojen käsittely on yleisen tietosuoja-asetuksen mukaan hyväksyttyä, mikäli se perustuu rekisteröidyn suostumukseen, sopimukseen, rekisterinpitäjän lakisääteinen velvoitteeseen, elintärkeiden etujen suojaamiseen, yleiseen etuun ja julkiseen valtaan tai rekisterinpitäjän tai kolmannen osapuolen oikeutettuun etuun. Käsittelyperuste täytyy määritellä ennen rekisteröidyn henkilötietojen keräämistä, eikä sitä voi myöhemmin muuttaa toiseksi. Käsittelyperuste vaikuttaa rekisteröidyn tietosuojaan liittyviin oikeuksiin. (Tietosuojavaltuutetun toimisto 2024i.)

2.2.1 Rekisteröidyn suostumus

Rekisteröidyn suostumuksen henkilötietojensa käsittelylle tulee olla vapaaehtoinen, yksilöity ja tietoisesti tehty. Suostumusta tulee kysyä rekisteröidyltä erikseen jokaista ennalta määriteltyä henkilötietojen käyttötarkoitusta varten. Suostumus pitää olla myös helposti peruutettavissa. (Andreasson ym. 2023, 182.) Vaikeneminen, esitäytetty rasti ruudussa tai jonkin asian tekemisen välistä jättäminen ei ole suostumuksen antamista. Suostumuksen pyytämistä on esimerkiksi opiskelupaikan hakijalta luvan kysyminen hänen nimensä julkaisun sallimiseen opiskelijavalinnan hyväksyttyjen listalla oppilaitoksen nettisivuilla. (Krakau & Haapalehto 2020, 199.)

Rekisterinpitäjän tulee pystyä osoittamaan jälkikäteen, milloin rekisteröity on antanut suostumuksensa ja mitä tietoa hänelle on annettu suostumuksen yhteydessä. Suostumuspyyntö tulee esittää myös mahdollisimman helposti ymmärrettävällä kielellä, eikä se saa sisältää rekisteröidyn kannalta epäreiluja ehtoja. (Hanninen ym. 2017, 38–39.) Mikäli rekisterinpitäjä käsittelee arkaluontoisia

henkilötietoja, siirtää henkilötietoja kolmansiin maihin tai tekee tiedoille automatisoituja yksittäispäätöksiä, täytyy rekisterinpitäjän pyytää tähän rekisteröidyltä nimenomainen suostumus. Nimenomainen suostumus voi olla esimerkiksi kirjallinen tai sähköinen allekirjoitus tai kaksivaiheinen varmistus, jossa rekisteröity tunnistautuu käyttäjätunnuksen lisäksi esimerkiksi tekstiviestitse lähetettävän koodin avulla. (Tietosuojavaltuutetun toimisto 2024e.)

2.2.2 Sopimus

Sopimukseen kuuluva rekisteröidyn henkilötietojen käsittely on tarpeen silloin kun se tarvitaan sopimuksen täytäntöön panemiseksi. Ennen sopimuksen tekemistä henkilötietojen käsittely, kuten henkilön nimen ja osoitteen säilyttäminen kohtuullisen ajan verran, on sallittua silloin kun henkilö pyytää yritystä lähettämään tarjouksen palvelusta tai tuotteesta. (Hanninen ym. 2017, 30.) Esimerkkejä sopimukseen perustuvasta henkilötietojen käsittelystä ovat tilanteet, joissa verkkokaupat käsittelevät asiakkaiden tietoja toimittaakseen tehdyt tilaukset perille, sähkösopimukset, joissa sähköfirmat tarvitsevat asiakkaiden yhteystiedot laskutusta varten tai työsopimukset, joissa työnantaja käsittelee työntekijän tietoja työsopimuksen perusteella. Työnantaja saa käsitellä työntekijän työsuhteen kannalta vain olennaisia tietoja. Tietosuojasäännösten lisäksi työntekijöiden henkilötietojen käsittelyssä tulee noudattaa työelämän tietosuojalakia. (Krakau & Haapalehto 2020, 200.)

2.2.3 Rekisterinpitäjän lakisääteinen velvoite

Henkilötietojen käsittely voi perustua rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseen. Tämä tarkoittaa sitä, että peruste käsittelylle löytyy Suomen kansallisesta lainsäädännöstä tai Euroopan unionin lainsäädännöstä. Lakisääteiset rekisterinpitäjän velvoitteet koskevat niin yksityisellä kuin myös julkisella puolella toimivia organisaatioita. (Korpisaari ym. 2022, 120.) Esimerkiksi työnantajan tulee kertoa työntekijänsä palkkatiedot veroviranomaisille, sairaalan täytyy ylläpitää potilasrekisteriä ja yhdistyslain mukaisesti yhdistyksen täytyy kerätä yhdistyksen jäsenten nimet ja kotipaikat jäsenluetteloon (Krakau & Haapalehto 2020, 201).

2.2.4 Elintärkeiden etujen suojaaminen

Silloin kun rekisteröity tai muu henkilö on vaarassa, on henkilötietojen käsittely hyväksyttyä elintärkeiden etujen suojaamiseksi. Elintärkeiden etujen turvaamiseen liittyvät tilanteet voivat olla esimerkiksi olosuhteita, joissa henkilön fyysisen koskemattomuus on vaarantunut tai on kyse elämästä ja kuolemasta. Esimerkiksi epidemian seuraamiseen liittyvissä tilanteissa sekä luonnonkatastrofien yhteyksissä henkilötietojen käsittely voi olla perusteltua elintärkeiden etujen suojaamiseksi. (Krakau & Haapalehto 2020, 201.)

2.2.5 Yleinen etu ja julkinen valta

Henkilötietojen käsittely on sallittua julkisella tai yksityisellä sektorilla tilanteissa, joissa yleinen etu tai rekisterinpitäjän julkinen valta sallii sen. Yleisen edun ja julkisen vallan peruste henkilötietojen käsittelylle tulee kuitenkin pohjautua lakiin tai muuhun oikeudelliseen säännökseen. Henkilötietojen yleisen edun käsittelyn perusteena voi olla esimerkiksi historiallinen tai tieteellinen tutkimus. (Andreasson ym. 2023, 183.) Muun muassa viranomaisten suorittamat suunnittelu- ja selvitystehtävät, sukututkimukset ja henkilötietojen luovuttamiset tilastointia varten ovat esimerkkejä yleisen edun ja julkisen vallan käsittelyperusteista (Krakau & Haapalehto 2020, 202).

2.2.6 Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Henkilötietojen käsittelyn perusteena voidaan käyttää oikeutettua etua esimerkiksi silloin kun muita edellä mainittuja käsittelyperusteita ei voi hyödyntää, ja se on tarpeen rekisterinpitäjän tai kolmannen osapuolen etujen toteuttamiseksi. Henkilötietojen käsittelyn perusteena voidaan käyttää oikeutettua etua esimerkiksi silloin kun rekisteröidyn ja rekisterinpitäjän välillä on jokin merkitsevä suhde, kuten asiakas- tai työsuhde. Rekisterinpitäjän tulee kuitenkin arvioida, onko sen mahdollista käyttää oikeutettua etua käsittelyn perusteena tasapainotestillä. Silloin kun henkilötietojen käsittely perustuu oikeutettuun etuun, on rekisteröidyllä milloin tahansa oikeus vastustaa henkilötietojensa käsittelyä. (Tietosuojavaltuutetun toimisto 2024j.) Esimerkkejä oikeutetun edun tilanteista ovat työntekijän lähiomaisen yhteystietojen säilyttäminen hätätilanteita silmällä pitäen, kaupan tallentava valvontakamera omaisuuden suojaamisen varalta tai henkilötietojen siirtäminen uuteen järjestelmään konsernin sisällä (Krakau & Haapalehto 2020, 202).

Tasapainotestillä rekisterinpitäjä tai kolmas osapuoli pohtii menevätkö heidän etunsa rekisteröidyn oikeuksien ja etujen edelle. Rekisteröidyn edut ja oikeudet ovat alustavasti suojatumpia kuin rekisterinpitäjän tai kolmannen osapuolen edut. Tasapainotestissä pohditaan kuuden kysymyksen avulla, onko oikeutettua etua mahdollista käyttää henkilötietojen käsittelyn perusteena. Tasapainotestin kysymyksissä pohditaan muun muassa onko oikeutettu etu oikeasti sopivin käsittelyperuste kaikista mahdollisista käsittelyperusteista huomioiden rekisteröidyn edut ja oikeudet. (Tietosuojavaltuutetun toimisto 2024j.)

2.2.7 Erityisten henkilötietoryhmien käsittely

Erityisiä henkilötietoryhmiä eli arkaluontoisia tietoja, kuten ammattiliiton jäsenyyttä tai terveyttä koskevia tietoja, ei pääsääntöisesti saa käsitellä ollenkaan, jos siihen ei ole jokin hyväksyttävä peruste. Rekisteröidyn nimenomaisella suostumuksella rekisterinpitäjä voi käsitellä arkaluontoisia henkilötietoja yhtä tai useampaa käyttötarkoitusta varten, ellei lainsäädäntö estä tätä yksiselitteisesti. Esimerkiksi laki yksityisyydestä työelämässä säätää, että työnantaja saa käsitellä vain tietoja,

jotka liittyvät työntekijän oikeuksien ja velvollisuuksien hoitamiseen. Tästä syystä työnantaja ei voi käsitellä työntekijän etnistä alkuperää koskevia tietoja, edes työntekijän nimenomaisella suostumuksella, koska etninen alkuperä ei vaikuta työntekijän oikeuksiin ja velvollisuuksiin. Toisaalta esimerkiksi HR-vastaavilla ja esihenkilöillä on tyypillisesti oikeus käsitellä työntekijän terveystietoja, kun se on tarpeen vaikkapa työstä poissaolemisen selvittämiseksi ja työntekijä on itse tuonut sairaspoissaolotodistuksen heille. (Hanninen ym. 2017, 41–44.)

Mikäli asiakkaiden arkaluontoisten henkilötietojen käsittely on tarpeellista organisaatiossa, niin tietojen käsittelyyn ja esimerkiksi säilyttämiseen tulee pyytää asiakkaiden suostumus. Ongelmia voi syntyä silloin kun joistakin tiedoista voi välillisesti käydä ilmi asiakkaan arkaluontoisia tietoja. Esimerkiksi erityisruokavaliosta voi päätellä henkilön terveydentilaan liittyviä tietoja. Jos tällaisia tietoja tallennetaan pysyvästi asiakasrekisteriin, kannattaa tähän ehdottomasti pyytää rekisteröidyltä suostumus. Mikäli yrityksessä käsitellään arkaluontoisia tietoja, joiden käsittelyyn ei ole asiakkailta lupaa, ne pitää poistaa välittömästi tai pyytää rekisteröidyiltä lupa jälkikäteen. (Hanninen ym. 2017, 42.)

2.3 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Rekisterinpitäjä on aina viime kädessä vastuussa sekä omasta, että henkilötietojen käsittelijöiden lainmukaisesta tietojen käsittelystä. Rekisterinpitäjän velvollisuutena on huolehtia, että sen käyttämät henkilötietojen käsittelijät käsittelevät henkilötietoja tietosuojasäädöksiä noudattaen. Rekisterinpitäjän kuuluu myös huolehtia organisaation teknisistä ja organisatorisista toimenpiteistä, kuten tietoturvasta, joilla varmistetaan henkilötietojen turvallinen käsittely. Rekisterinpitäjän täytyy lisäksi ottaa henkilötietojen käsittelyssä huomioon mahdolliset riskit, joita voi aiheutua rekisteröidyn oikeuksille ja vapauksille. Varsinkin arkaluonteisten henkilötietojen ja lasten henkilötietojen käsittelyssä on hyvä olla tarkkana. (Hanninen ym. 2017, 26–27.)

Henkilötietojen käsittelijä ei saa yleisen tietosuoja-asetuksen mukaan itsenäisesti määritellä rekisterinpitäjän lukuun käsittelemiensä henkilötietojen käsittelyn tarkoituksia. Jos henkilötietojen käsittelijä tekee näin, niin se katsotaan rekisterinpitäjäksi, jolloin sitä koskevat kaikki rekisterinpitäjän velvollisuudet. Rekisterinpitäjän velvollisuuksia ovat muun muassa osoitusvelvollisuus ja velvollisuus vastata rekisteröityjen pyyntöihin tietojensa käsittelyyn liittyviin kysymyksiin. Henkilötietojen käsittelijä saa käyttää käsittelyssä alihankkijoita, mikäli rekisterinpitäjä on antanut siihen luvan. Myös alihankkijoiden täytyy noudattaa toimissaan tietosuojasäännöksiä ja toimia rekisterinpitäjän määrittämällä tavalla. (Hanninen ym. 2017, 27–28.)

Rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja velvollisuudet on määritelty yleisessä tietosuoja-asetuksessa. Rekisterinpitäjän tehtävänä on siis määritellä henkilötietojen käsittelyn

tarkoitukset ja keinot. Henkilötietojen käsittelijä puolestaan käsittelee henkilötietoja rekisterinpitäjän antamien ohjeiden mukaisesti. (Hanninen ym. 2017, 24.) Rekisterinpitäjän ja henkilötietojen käsittelijän yleisiä velvollisuuksia ovat muun muassa sisäänrakennetun ja oletusarvoisen tietosuojan omaksuminen, selosteen tekeminen käsittelytoimista ja yhteistyö valvontaviranomaisten kanssa (Korpisaari ym. 2022, 297). Tässä luvussa käsitellään rekisterinpitäjän ja henkilötietojen käsittelijän keskinäisiä velvollisuuksia sekä yhteisrekisterinpitäjyyttä.

2.3.1 Läpinäkyvyys ja jäljitettävyys

Rekisterinpitäjän täytyy laatia henkilötietojen käsittelijän kanssa sopimus, josta selviää kummankin osapuolen velvollisuudet ja muut tiedot yleisen tietosuoja-asetuksen artiklan 28 mukaisesti. Henkilötietojen käsittelijän täytyy myös luoda rekisterinpitäjän henkilötietojen käsittelyn ohjeista kirjalliset dokumentit, jotta henkilötietojen käsittelijä voi osoittaa toimivansa rekisterinpitäjän ohjeiden mukaisesti. Mikäli henkilötietojen käsittelijä haluaa käyttää henkilötietojen käsittelyssä apuna muita käsittelijöitä, tähän täytyy saada kirjallinen lupa rekisterinpitäjältä. Henkilötietojen käsittelijän tulee tarvittaessa toimittaa kaikki tiedot rekisteripitäjälle, jotka tarvitaan henkilötiedon käsittelijän tietosuojan tason selvittämiseen. Henkilötietojen käsittelijän tulee tarvittaessa myös tehdä seloste käsittelytoimista. (Tietosuojavaltuutetun toimisto 2024k.) Seloste käsittelytoimista on organisaation oma dokumentti, jossa kerrotaan, miten organisaatiossa käsitellään henkilötietoja tietosuojasäädösten mukaisesti (Andreasson & Ylipartanen 2022, 186).

2.3.2 Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet

Sisäänrakennetulla ja oletusarvoisella tietosuojalla (privacy by design ja privacy by default) tarkoitetaan näkökulmaa, jossa tietosuojan periaatteiden toteutuminen huomioidaan henkilötietojen käsittelyssä alusta alkaen esimerkiksi organisaation, palvelun tai sovelluksen toiminnassa. Eli tietosuojaan ja yksityisyyteen liittyvät vastuut huomioidaan henkilötietojen käsittelyssä suunnitteluvaiheesta aina tietojen poistamiseen saakka. Toisin sanoen tietosuojan huomioiminen ei ole pelkästään esimerkiksi tietosuojavastaavan vastuulla, vaan kaikkien niiden henkilöiden, joiden työhön liittyy henkilötietojen käsittelyä tai käsittelyn suunnittelua. (Korpisaari ym. 2022, 310–311.)

Henkilötietojen käsittelijän tulee taata rekisterinpitäjälle, että rekisteröityjen henkilötietojen käsittely tapahtuu tietosuoja-asetusten vaatimusten mukaisesti. Henkilötietojen käsittelijä voi osoittaa tämän esimerkiksi siten, että sen tuotteissa tai palveluissa ei kerätä turhia henkilötietoja, ja tiedot poistetaan rekisteröityjen pyynnöstä tai kun ne käyvät tarpeettomiksi. Toisin sanoen rekisterinpitäjälle tarjottavien palvelujen ja työkalujen tulisi noudattaa tietosuojaperiaatteita ja oletusarvoisesti kohdistaa henkilötietojen käsittely vain tarpeellisiin tietoihin. (Tietosuojavaltuutetun toimisto 2024k.)

2.3.3 Henkilötietojen käsittelijän suojaamisvelvoite sekä rekisterinpitäjän avustus

Rekisterinpitäjän ja henkilötietojen käsittelijän alaiset ovat salassapitovelvollisia, mikäli heillä on oikeus käsitellä henkilötietoja. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee huolehtia tietojen turvallisesta käsittelystä esimerkiksi riittävällä tietoturvan laadulla. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksista rekisterinpitäjälle heti sellaisen sattuessa. Henkilötietojen käsittelijän palvelun loputtua sen täytyy palauttaa kaikki käsittelemänsä tiedot rekisterinpitäjälle tai hävittää ne rekisterinpitäjän ohjeita noudattaen. (Tietosuojavaltuutetun toimisto 2024k.)

Mikäli rekisterinpitäjän antamat ohjeet henkilötietojen käsittelijälle eivät ole tietosuojasäädösten mukaisia, niin tästä tulee ilmoittaa välittömästi rekisterinpitäjälle. Henkilötietojen käsittelijä on velvollinen myös avustamaan rekisterinpitäjää tilanteissa, joissa rekisteröidyt käyttävät oikeuksiaan. Esimerkiksi jos rekisteröity pyytää nähtäväksi kaikkia tietoja, mitä heistä on tallennettu, niin henkilötietojen käsittelijän täytyy antaa tai avustaa näiden tietojen välittämisessä rekisteröidylle. Henkilötietojen käsittelijän tulee myös avustaa rekisterinpitäjää tietojen käsittelyn turvallisuuteen liittyvissä asioissa, tietoturvaloukkauksen ilmoittamisissa ja vaikutustenarvioinneissa tietosuojaan liittyen. (Tietosuojavaltuutetun toimisto 2024k.)

2.3.4 Yhteisrekisterinpitäjyys

Yhteisrekisterinpitäjien, eli kahden tai useamman organisaation tulee yhdessä määritellä omat vastuualueensa henkilötietojen käsittelyssä sekä rekisteröityjen oikeuksien toteuttamisesta ja rekisteröityjen tiedottamisesta. Yhteisrekisterinpitäjien roolit, vastuualueet ja järjestelyt näiden suhteen tulee olla rekisteröityjen saatavilla esimerkiksi tietosuojaselosteen muodossa. Tärkeää olisi esimerkiksi määritellä kehen yhteisrekisterinpitäjistä rekisteröityjen tulisi ensisijaisesti olla tarvittaessa yhteydessä. (Hanninen ym. 2017, 28.)

2.4 Tietosuojavastaavan rooli

Tietosuojavastaavan nimittämisestä, asemasta ja tehtävistä säädetään yleisessä tietosuoja-asetuksessa 37-39 artikloissa (yleinen tietosuoja-asetus). Rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee olla tietoisia siitä, tarvitaanko yleisen tietosuoja-asetuksen mukaan heidän organisaatiossansa tietosuojavastaavaa. Tietosuojavastaava tulee nimittää silloin kun organisaatio käsittelee henkilötietoja laajamittaisesti, säännöllisesti ja järjestelmällisesti tai käsittely kohdistuu erityisiin henkilötietoryhmiin. (Andreasson & Ylipartanen 2022, 104.)

Tietosuojavastaavan tehtävänä on valvoa, että organisaatiossa henkilötietoja käsitellään tietosuojasäädösten vaatimalla tavalla. Tietosuojavastaava on myös henkilö, kehen rekisteröidyt voivat olla yhteydessä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaavan toimenkuvaan

kuuluu myös organisaation työntekijöiden ja johdon neuvonta tietosuojan toteuttamisessa. Lisäksi tietosuojavastaava toimii yhteyshenkilönä organisaation ja valvontaviranomaisten välillä tietosuojaan liittyvissä asioissa. Vaikka tietosuojavastaava valvoo ja ohjeistaa organisaation toimintaa tietosuojan osalta, vastuu henkilötietojen käsittelyn lainmukaisuudesta kuuluu silti johdolle. (Andreasson & Ylipartanen 2022, 104.)

2.4.1 Tietosuojavastaavan työnkuva, tehtävät ja asema

Tietosuojavastaavan tärkeimpänä tehtävänä organisaatiossa on yleisen tietosuoja-asetuksen ja muun tietosuojaan liittyvän lainsäädännön asiantuntijana toimiminen. Tietosuojavastaavan tulee siksi seurata aktiivisesti muuttuvia tietosuojaohjeistuksia ja lainsäädäntöä, jotta hän voi tiedottaa mahdollisista tietosuojaan liittyvistä muutostarpeista organisaatiossa. Tietosuojavastaavan tulee myös valvoa ja seurata huolellisesti rekisteröityjen oikeuksien toteutumista. Hänen tulee myös pitää huoli siitä, että rekisteröidyt saavat neuvontaa ja ohjausta aina tarvittaessa. Tietosuojavastaavan tulee myös varmistaa, että rekisteröidyt ovat mahdollisimman hyvin perillä oikeuksistaan liittyen heidän henkilötietojen käsittelyyn liittyviin asioihin. (Andreasson & Ylipartanen 2022, 107.)

Tietosuojavastaavan tehtäviin kuuluu työntekijöiden ja johdon ohjeistaminen, neuvonta ja kouluttaminen tietosuojaan liittyvissä asioissa organisaation sisällä. Osoitusvelvollisuuden vuoksi tietosuojavastaava työhön kuuluu henkilötietojen käsittelyyn liittyvän dokumentaation laatimista, saatavuuden varmistamista sekä säilyttämistä. Tietosuojavastaavan tulee myös tukea organisaation eri yksiköitä tietosuojariskien havaitsemisessa ja auttaa yksiköitä riskien hallitsemisessa. Tietoturvaloukkauksen sattuessa tietosuojavastaava valvoo, että loukkauksesta ilmoitetaan valvontaviranomaisille. (Andreasson & Ylipartanen 2022, 108–109.)

Tietosuojavastaavaa ei saa ottaa työssään sellaisia ohjeita vastaan, joilla yritettäisiin vaikuttaa hänen päätöksiinsä, valvontatyöhön tai tulkintaan tietosuojasäädöksistä, vaan hänen asemansa tulee olla riippumaton. Tietosuojavastaavaa ei saa rangaista siitä, että hän hoitaa tehtäviään. Suosituksena on, että mikäli organisaatiossa päädytään toimimaan tietosuojavastaavan neuvojen vastaisesti, tämä perustellaan kirjallisesti. Tietosuojavastaavalle tulisi myös taata riittävät resurssit työstään suoriutumiseen. Tietosuojavastaava tulisi aina ottaa ajoissa mukaan arvioimaan esimerkiksi uusien tietojärjestelmien hankintaa tai projektien suunnittelua, jos niissä on tarpeen arvioida henkilötietojen käsittelyn vaatimuksia yleisen tietosuojasäädösten näkökulmasta. Tietosuojavastaavan tulee myös raportoida ylimmälle johdolle organisaation tietosuojan tilasta. (Andreasson & Ylipartanen 2022, 109–110.)

2.4.2 Tietosuojavastaavan toiminta henkilöstön tukena

Onnistukseen mahdollisimman hyvin tehtävässään tietosuojavastaava tarvitsee taakseen johdon tuen. On tärkeää, että johto ymmärtää tietosuojan olevan yksi osa organisaation kokonaisturvallisuutta, josta johto on vastuussa. Johdon omistautuminen tietosuojan yllä pitämiseen on ensiarvoisen tärkeää, jotta tietosuojavastaava pystyy toimimaan organisaation henkilöstön tukena tietosuoja-asioissa mahdollisimman onnistuneesti. (Andreasson & Ylipartanen 2022, 125.)

Tietosuojavastaavan tehtäviin kuuluu tietosuoja-asiantuntijana toimimisen lisäksi neuvojen antaminen ja koulutuksen järjestäminen. Uusia työntekijöitä perehdyttäessä tietosuojaan liittyvistä asioista ja toimintatavoista on hyvä järjestää koulutusta jo työuran alkumetreillä organisaatiossa. Työntekijöiden tietosuojaosaamisen parantamiseen hyviä apukeinoja ovat tietoturva- ja tietosuojaoppaat, kvartaaleittain ilmestyvät tiedottavat lehtiset intranetissä tai sähköpostissa, verkkokurssit, luentokoulutukset, erilaiset pelit ja pulmat, säännölliset lyhyet pikaohjeet ja julisteet, tapahtumat, teemapäivät, kampanjat sekä lyhyet videot, joissa esiintyisivät mielellään myös johtoryhmän jäseniä. (Andreasson & Ylipartanen 2022, 131–136.)

2.5 Rekisteröidyn oikeudet

Yleisen tietosuoja-asetuksen ydinideana on se, että jokaisella yksilöllä on oikeus omien henkilötietojensa suojaan, turvalliseen ja lainmukaiseen käsittelyyn sekä hallintaan. Kun rekisteröidyn tietoja käsitellään, on sille oltava jokin tietty tarkoitus ja laillinen peruste, kuten rekisteröidyn suostumus. Rekisteröidylle käsittelyn oikeusperuste tulee kertoa esimerkiksi tietosuojaselosteessa. Rekisteröidyn oikeuksia ovat oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada tutustua tietoihin, oikeus oikaista tietoja, oikeus poistaa tiedot ja tulla unohdetuksi, oikeus rajoittaa tietojen käsittelyä, oikeus siirtää tiedot järjestelmästä toiseen, oikeus vastustaa tietojen käsittelyä ja oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. Rekisteröity ei kuitenkaan välttämättä pysty käyttämään kaikkia oikeuksiaan, koska niiden käyttöön vaikuttaa rekisterinpitäjän määrittelemä henkilötietojen käsittelyn oikeusperuste. Tämän vuoksi rekisterinpitäjän tulee miettiä tarkkaan, mitä perustetta se käyttää henkilötietojen käsittelyperusteena. (Andreasson ym. 2023, 51.)

Rekisterinpitäjän tulee kertoa rekisteröidylle helposti ja ymmärrettävällä tavalla, miten ja mihin tarkoitukseen hänen henkilötietojansa käsitellään organisaatiossa. Yksi yleiseksi muodostunut tapa tietojen kertomiseksi on tietosuojaseloste organisaation verkkosivuilla. Tietosuojaselosteessa tulee kertoa muun muassa rekisteröidyn oikeuksista ja kuinka niitä voi käyttää, henkilötietojen käsittelyn tarkoitukset, oikeusperuste kutakin käsittelyn tarkoitusta varten, tieto mistä henkilötiedot on saatu, henkilötietojen vastaanottajat, jos tietoja luovutetaan muille käsittelijöille ja tieto siitä, kuinka kauan henkilötietoja käsitellään. Tietosuojaseloste on hyvä tapa toteuttaa yleisen tietosuoja-asetuksen

läpinäkyvyysperiaatetta sekä sisäänrakennetun ja oletusarvoisen tietosuojan edellytystä. (Andreasson ym. 2023, 187–188.)

2.5.1 Oikeus saada tietoa henkilötietojen käsittelystä

Henkilötietojen käsittelyn tulee olla läpinäkyvää. Tämän vuoksi rekisteröidyllä on oikeus saada tietää, kuinka hänestä kerätään tietoja ja miten niitä käsitellään. Rekisteröidylle täytyy kertoa esimerkiksi rekisterinpitäjän yhteystiedot, käsittelyn tarkoitukset, tietojen käsittelyperuste, tietojen käsittelyajoista, luovutetaanko tai siirretäänkö tietoja EU:n ja ETA-alueen ulkopuolelle, rekisteröidyn oikeuksista sekä mistä tiedot on saatu, jos ne on saatu muualta kuin rekisteröidyltä. Rekisteröidylle tulee kertoa henkilötietojensa käsittelystä helposti ymmärrettävällä kielellä esimerkiksi helposti saatavilla olevan tietosuojaselosteen muodossa. (Tietosuojavaltuutetun toimisto 2024l.)

Rekisteröityä tulee informoida tietojen keräämisen yhteydessä oikeudesta saada tietoa henkilötietojensa käsittelystä esimerkiksi tietosuojaselosteen avulla. Jos rekisteröidyn tiedot on saatu muualta kuin häneltä itseltään, täytyy rekisteröityä informoida viimeistään kuukauden kuluttua tietojen saamisesta. Jos muualta saatuja rekisteröidyn tietoja käytetään viestintään, niin häntä täytyy informoida asiasta silloin kun häneen ollaan ensimmäisen kerran yhteyksissä. Kun muualta saatuja tietoja luovutetaan ensimmäisen kerran toiselle vastaanottajalle, tästä täytyy informoida rekisteröityä. (Tietosuojavaltuutetun toimisto 2024l.)

Informointia rekisteröidylle ei kuitenkaan tarvitse tehdä silloin kun rekisteröityä on jo aikaisemmin informoitu asiasta. Rekisteröityä ei tarvitse silloinkaan informoida, kun hänen tietonsa on saatu muualta ja informointi osoittautuisi äärimmäisen vaikeaksi tai siitä aiheutuva vaiva olisi kohtuuton. Muita syitä jättää rekisteröity informoimatta on muun muassa yleiseen turvallisuuteen, rikosten ennaltaehkäisyyn ja verotuksen valvontaan liittyvien asioiden takia. Lisäksi joissain tapauksissa rekisteröityä ei tarvitse informoida yleisen edun, oikeutetun edun tai laissa säädetyn informoitavia koskevan vaitiolovelvollisuuden vuoksi. (Tietosuojavaltuutetun toimisto 2024l.)

2.5.2 Oikeus saada tutustua tietoihin

Rekisteröidyllä on oikeus saada tietää mitä tietoja rekisterinpitäjällä on hänestä kerättynä. Rekisteröity voi halutessaan pyytää rekisterinpitäjää lähettämään kaikki hänestä kerätyt tiedot itselleen. Jos rekisteröity tekee pyynnön sähköisesti, rekisterinpitäjän tulee toimittaa tiedot rekisteröidylle sähköisesti, ellei rekisteröity erikseen pyydä toista toimitusmuotoa tiedoille. (Tietosuojavaltuutetun toimisto 2024m.)

Rekisteröidyn pyyntöön tietojen lähettämisestä tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Mikäli rekisterinpitäjä tarvitsee tietojen lähettämiseen enemmän

aikaa, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan se ilmoittaa määräajan pidentämisestä perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy lähettämästä rekisteröidylle tietoja, tästä tulee ilmoittaa hänelle kuukauden kuluessa. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä asiassa valvontaviranomaisen puoleen. (Tietosuojavaltuutetun toimisto 2024m.)

Rekisterinpitäjä voi kieltäytyä lähettämästä rekisteröidylle tietoja, jos sille on lainmukainen peruste. Lainmukainen peruste voisi olla esimerkiksi se, että pyyntöjä esitetään toistuvasti, tietojen lähettäminen voisi vaarantaa rekisteröidyn terveyden tai oikeudet, tietojen lähettäminen voisi haitata yleistä turvallisuutta tai rikosten ehkäisyä. Mikäli rekisterinpitäjä epäilee tietoja pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. (Tietosuojavaltuutetun toimisto 2024m.)

2.5.3 Oikeus oikaista tietoja

Rekisteröidyllä on oikeus vaatia rekisterinpitäjältä oikaisua virheellisiin tietoihin sekä täydennystä puutteellisiin henkilötietoihin. Oikaisupyynnön tekemisen tulisi lähtökohtaisesti olla maksutonta. Rekisterinpitäjän tulee ilmoittaa henkilötietojen oikaisuista jokaiselle taholle, kelle rekisteröidyn tietoja on luovutettu. (Tietosuojavaltuutetun toimisto 2024n.)

Rekisteröidyn pyyntöön tietojen oikaisuista tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Vastauksessa rekisterinpitäjän tulee kertoa, minkälaisiin toimiin se on ryhtynyt tietojen korjaamiseksi. Mikäli rekisterinpitäjä tarvitsee tietojen oikaisuun enemmän aikaa kuin kuukauden, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan määräajan pidentämisestä ilmoitetaan perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy oikaisemasta tietoja, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa rekisteröidyn oikaisupyynnöstä. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä valvontaviranomaisen puoleen tarvittaessa. (Tietosuojavaltuutetun toimisto 2024n.)

Rekisterinpitäjä voi kieltäytyä oikaisemasta tietoja, jos rekisteröidyn oikaistavaksi haluamat tiedot ovat henkilötietojen käsittelyn tarkoituksen kannalta puutteellisia tai virheellisiä. Mikäli rekisterinpitäjä epäilee tietoja pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. (Tietosuojavaltuutetun toimisto 2024n.)

2.5.4 Oikeus poistaa tiedot eli tulla unohdetuksi

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan kaikki tiedot hänestä, ja ”tulla unohdetuksi”. Tietojen poistamisesta tulee ilmoittaa myös jokaiselle taholle, jolle rekisteröidyn tietoja on

luovutettu. Rekisteröidyn tiedot pitää poistaa muun muassa silloin kun henkilötietoja ei enää tarvita sitä tarkoitusta varten minkä vuoksi ne alun perin kerättiin, rekisteröity peruuttaa suostumuksensa tietojen käsittelyn perusteesta, rekisteröity ei halua hänen tietojaan käytettävän suoramarkkinointiin tai henkilötietojen käsittelylle ei ole lainmukaista perustetta. (Tietosuojavaltuutetun toimisto 2024o.)

Rekisteröidyn pyyntöön tietojen poistamisesta tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Vastauksessa rekisterinpitäjän tulee kertoa, minkälaisiin toimiin se on ryhtynyt tietojen poistamiseksi. Mikäli rekisterinpitäjä tarvitsee tietojen poistoon enemmän aikaa kuin kuukauden, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan määräajan pidentämisestä ilmoitetaan perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy poistamasta tietoja, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa rekisteröidyn oikaisupyynnöstä. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä valvontaviranomaisen puoleen tarvittaessa. (Tietosuojavaltuutetun toimisto 2024o.)

Rekisterinpitäjä voi kieltäytyä tietojen poistosta tietyissä tilanteissa. Tällaisia tilanteita ovat esimerkiksi olosuhteet, joissa tietojen poiston seurauksena sananvapauden ja tiedonvälityksen vapautta koskeva oikeus voisi vaarantua, kansanterveyteen liittyvä yleinen etu olisi uhattuna, yleisen edun mukainen arkistointitarkoitus tai tieteellinen tutkimustarkoitus vaikeutuisi tai oikeudellinen prosessi vaarantuisi. Mikäli rekisterinpitäjä epäilee tietoja pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. (Tietosuojavaltuutetun toimisto 2024o.)

2.5.5 Oikeus rajoittaa tietojen käsittelyä

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää rajoittamaan henkilötietojensa käsittelyä. Rajoitettuja henkilötietoja saa säilyttämisen lisäksi käsitellä vain rekisteröidyn suostumuksella, oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi, toisen henkilön oikeuksien suojaamiseksi tai EU:n yleistä etua koskevan syyn takia. Rekisteröidyllä on oikeus vaatia tietojensa käsittelyn rajoittamista silloin kun hän kiistää henkilötietojensa paikkansapitävyyden, käsittely on lainvastaista, mutta rekisteröity vastustaa tietojen poistamista, rekisteröity tarvitsee tietojensa käsittelyn rajoittamista oikeudellisen syyn takia tai rekisteröity on vastustanut henkilötietojensa käsittelyn siksi aikaa, kun selvitetään syrjäyttävätkö rekisterinpitäjän edut rekisteröidyn edut. Rekisteröidyn henkilötietojen käsittelyä voidaan rajoittaa esimerkiksi poistamalla hänen tietonsa julkiselta verkkosivulta. (Tietosuojavaltuutetun toimisto 2024p.)

Rekisteröidyn pyyntöön tietojen käsittelyn rajoittamisesta tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Vastauksessa rekisterinpitäjän tulee kertoa, minkälaisiin toimiin se on ryhtynyt tietojen käsittelyn rajoittamiseksi. Mikäli rekisterinpitäjä tarvitsee tietojen

käsittelyn rajoittamiseen enemmän aikaa kuin kuukauden, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan määräajan pidentämisestä ilmoitetaan perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy rajoittamasta tietojen käsittelyä, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa rekisteröidyn oikaisupyynnöstä. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä valvontaviranomaisen puoleen tarvittaessa. Rekisteröidylle on ilmoitettava ennen kuin tietojen käsittelyyn vaikuttava rajoitus poistetaan. (Tietosuojavaltuutetun toimisto 2024p.)

Rekisterinpitäjä voi kieltäytyä tietojen käsittelyn rajoittamisesta, jos siihen ei ole rekisterinpitäjän mielestä oikeudellisia perusteita tai tieteellinen tai historiallinen tutkimustarkoitus vaarantuisi. Mikäli rekisterinpitäjä epäilee henkilötietojen käsittelyn rajoittamista pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. Rekisterinpitäjän tulee ilmoittaa jokaiselle taholle tietojen käsittelyn rajoittamisesta, kelle tietoja on luovutettu. (Tietosuojavaltuutetun toimisto 2024p.)

2.5.6 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada rekisterinpitäjälle antamansa henkilötiedot takaisin ja siirtää tiedot toiselle rekisterinpitäjälle. Rekisteröidyllä on myös oikeus vaatia rekisterinpitäjää siirtämään kyseiset tiedot toiselle rekisterinpitäjälle suoraan, jos se on teknisesti mahdollista. Rekisteröity voi käyttää oikeutta tietojen siirtoon järjestelmästä toiseen silloin kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen. Rekisterinpitäjää ei kuitenkaan voida vaatia siirtämään tietoja, jotka se on itse tuottanut ja analysoinut rekisteröidyn tarkkailun tai hänen antamien tietojen perusteella. (Tietosuojavaltuutetun toimisto 2024q.)

Rekisteröidyn pyyntöön tietojen siirtämisestä järjestelmästä toiseen tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Vastauksessa rekisterinpitäjän tulee kertoa, minkälaisiin toimiin se on ryhtynyt tietojen siirtämiseksi. Mikäli rekisterinpitäjä tarvitsee tietojen siirtämiseen enemmän aikaa kuin kuukauden, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan määräajan pidentämisestä ilmoitetaan perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy tietojen siirtämisestä toiseen järjestelmään, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa rekisteröidyn pyynnöstä. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä valvontaviranomaisen puoleen tarvittaessa. (Tietosuojavaltuutetun toimisto 2024q.)

Henkilötietoja vastaanottavan uuden rekisterinpitäjän tulee varmistaa, että toiselta rekisterinpitäjältä saadut tiedot ovat tarpeellisia sen käyttötarkoituksia varten. Mikäli näin ei ole, pitää tarpeettomat tiedot poistaa ja jättää käsittelemättä. Tämän vuoksi on tärkeää, että henkilötietoja vastaanottava rekisterinpitäjä ilmoittaa tietoja siirtävälle rekisterinpitäjälle henkilötietojen käsittelyn tarkoituksen ennen kuin tietojen siirtäminen tapahtuu. (Tietosuojavaltuutetun toimisto 2024q.)

Rekisterinpitäjä voi kieltäytyä tietojen siirtämisestä toiseen järjestelmään, jos siihen ei ole rekisterinpitäjän mielestä oikeudellisia perusteita, siirtäminen vaikuttaisi haitallisesti muiden oikeuksiin ja vapauksiin tai tutkimusaineistojen, kulttuuriperintöaineistojen sekä näiden kuvailutietojen sisältämien henkilötietojen käsittely arkistointitarkoituksessa vaarantuisi. Mikäli rekisterinpitäjä epäilee henkilötietojen käsittelyn rajoittamista pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. (Tietosuojavaltuutetun toimisto 2024q.)

2.5.7 Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä henkilökohtaisiin syihin vedoten silloin kun tietoja käsitellään yleistä etua koskevan asian saavuttamiseksi, rekisterinpitäjän julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmansien osapuolten oikeutettujen etujen toteuttamiseksi. Rekisterinpitäjän täytyy lopettaa tietojen käsittely, ellei se pysty perustelemaan hyvällä syyllä miksi käsittely syrjäyttäisi rekisteröidyn edut, oikeudet ja vapaudet. Rekisteröity voi vastustaa henkilötietojensa käyttöä suoramarkkinointiin ilman perusteluja, jolloin se tulee lopettaa. Rekisterinpitäjän ei tarvitse lopettaa käsittelyä silloin kun se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Tietosuojavaltuutetun toimisto 2024r.)

Rekisteröidyn pyyntöön tietojen käsittelyn lopettamisesta tulee vastata ilman viivytystä, kuitenkin enintään kuukauden kuluessa pyynnöstä. Vastauksessa rekisterinpitäjän tulee kertoa, minkälaisiin toimiin se on ryhtynyt tietojen käsittelyn lopettamiseksi. Mikäli rekisterinpitäjä tarvitsee tietojen käsittelyn lopettamiseen enemmän aikaa kuin kuukauden, niin määräaikaa on mahdollista jatkaa kahdella kuukaudella, kunhan määräajan pidentämisestä ilmoitetaan perustellusti rekisteröidylle. Jos rekisterinpitäjä kieltäytyy tietojen käsittelyn lopettamisesta, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa rekisteröidyn pyynnöstä. Rekisteröityä on myös neuvottava mahdollisuudesta kääntyä valvontaviranomaisen puoleen tarvittaessa. (Tietosuojavaltuutetun toimisto 2024r.)

Rekisterinpitäjä voi kieltäytyä tietojen käsittelyn lopettamisesta, jos siihen ei ole rekisterinpitäjän mielestä oikeudellisia perusteita. Tietojen käsittelyä ei välttämättä tarvitse lopettaa tieteellisen tai historiallisen tutkimuksen tai tilastoinnin yhteydessä tiettyjen edellytysten täyttyessä. Mikäli rekisterinpitäjä epäilee henkilötietojen käsittelyn rajoittamista pyytävän rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä. (Tietosuojavaltuutetun toimisto 2024r.)

2.5.8 Oikeus olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon, kuten profiloinnin, kohteeksi. Rekisteröity voi myös vaatia, että häntä koskevat päätökset tekee ihminen esimerkiksi

tilanteissa, joilla voi olla rekisteröidyn kannalta oikeudellisia vaikutuksia. Automaattisella päätöksenteolla tarkoitetaan toimintaa, jossa päätös perustuu ainoastaan automaattiseen henkilötietojen käsittelyyn. Automaattinen päätöksenteko voi perustua esimerkiksi rekisteröidyn täyttämän kyselylomakkeen tietoihin, puhelinsovelluksen keräämiin sijaintitietoihin sekä pääteltyyn tai tietyistä tiedoista johdettuun tietoon. (Tietosuojavaltuutetun toimisto 2024s.)

Rekisteröidyn oikeuteen olla joutumatta automaattisen päätöksenteon kohteeksi on kuitenkin olemassa poikkeuksia. Automaattinen päätöksenteko on hyväksyttyä, jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, päätös perustuu rekisteröidyn nimenomaiseen suostumukseen, automaattinen päätöksenteko on hyväksyttyä rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä. Mikäli rekisterinpitäjä käyttää toimissaan automaattista päätöksentekoa on sen huolehdittava, että rekisteröidylle kerrotaan tietojen käsittelyn tavoista, rekisteröidyillä on mahdollisuus vaatia ihmisen osallistumista tietojen käsittelemiseen, esittää oma näkökulma ja riitauttaa automaattisen päätöksenteon päätös. Rekisterinpitäjän on hyvä myös tarkistaa säännöllisesti, jotta automaattisen päätöksenteon prosessit toimivat kuten on suunniteltu, eikä ne vahingossa syrji ketään rekisteröityjen henkilötietojen perusteella. (Tietosuojavaltuutetun toimisto 2024s.)

Automaattista päätöksentekoa, kuten profilointia saa yleensä käyttää markkinointitarkoituksiin, silloin kun sillä ei ole merkittäviä esimerkiksi oikeudellisia vaikutuksia yksilöihin. Tämä riippuu kuitenkin profilointimenettelyn tunkeilevuudesta, markkinointikanavista, tavasta ja markkinoinnin kohteina olevien henkilöiden haavoittuvuudesta. Esimerkiksi korkeakorkoisten lainojen säännöllinen markkinointi taloudellisessa ahdingossa oleville voi johtaa lisävelkaantumiseen, jolloin markkinoinnilla voi olla merkittäviä vaikutuksia yksilön elämään. (Tietosuojavaltuutetun toimisto 2024s.)

2.6 Tietoturvaloukkaus ja valvontaviranomaisten toimivaltuudet

Henkilötietojen tietoturvaloukkauksesta on kyse silloin kun henkilötietoja häviää, tiedot muuttuvat tai tietoja päätyy henkilöille, joilla ei pitäisi olla oikeutta niihin. Tietoturvaloukkauksessa henkilötietojen käsittelijä tai rekisterinpitäjä voivat esimerkiksi hukata muistitikun tai työpuhelimen, lähettää lääkereseptin, potilaskertomuksen tai tiliotteen väärälle henkilölle tai lähettää suoramarkkinointiviestin sähköpostilla niin, että sen vastaanottajat voivat nähdä muiden sähköpostin saaneiden sähköpostiosoitteet. Myös tietomurrot, haittaohjelmatartunnat sekä henkilötietoja sisältävien tulosteiden unohtaminen tulostimeen muiden saataville ovat tietoturvaloukkauksia. (Korpisaari ym. 2022, 80–81.)

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee toimia parhaansa mukaan välttääkseen tietoturvaloukkaukset, koska niistä voi aiheutua rekisteröidyille fyysistä, aineellista, taloudellista tai sosiaalista vahinkoa. Tietoturvaloukkaukset voivat johtaa esimerkiksi identiteettivarkauksiin, petoksiin

tai mainehaittoihin. Tietoturvaloukkauksesta tulee myös ilmoittaa rekisteröidylle silloin kun arvioidaan, että organisatoriset ja tekniset toimenpiteet eivät riitä turvaamaan tietojen turvassa pysymistä tietoturvaloukkauksen jälkeen. (Andreasson & Ylipartanen 2022, 196–197.)

Tietosuojavaltuutetun toimisto toimii kansallisena tietosuojaviranomaisena Suomessa. Tietosuojavaltuutetun toimivaltuuksia ovat tutkintavaltuudet, hyväksymis- ja neuvontavaltuudet ja korjaavat toimivaltuudet, joita ovat esimerkiksi hallinnolliset seuraamusmaksut. Tietosuojavaltuutetun toimisto voi ottaa asioita käsiteltäväkseen esimerkiksi kantelun, ennakkokuulemisen, julkisuudessa olleiden tietojen tai tietoturvaloukkausilmoitusten kautta. Tietosuojavaltuutetun toimisto voi lähettää rekisterinpitäjälle tai henkilötietojen käsittelijälle selvityspyynnön, silloin kun se tutkii organisaation tietojenkäsittelyn lainmukaisuutta. (Andreasson & Ylipartanen 2022, 228.)

2.6.1 Tietoturvaloukkausten ilmoittamisprosessi ja dokumentointi

Mikäli organisaation työntekijä, palveluntarjoaja tai asiakas epäilee, että henkilötietojen käsittely ei ole täysin turvallista tai rekisteröityjen oikeudet ovat vaarantuneet, on heidän hyvä ilmoittaa havainnostaan rekisterinpitäjälle. Jokainen työntekijä on velvollinen ilmoittamaan havainnoistaan joko esihenkilöllensä tai suoraan tietosuojavastaavalle. Epäillyistä tietoturvaloukkauksista olisi suositeltavaa tehdä osoitusvelvollisuuden vuoksi alusta asti kattavat dokumentit, joista selviää muun muassa mitä on tapahtunut, kuinka montaa henkilöä tapahtunut koskettaa, ovatko rekisteröityjen arkaluontoiset tiedot vaarantuneet sekä milloin epäilty tietoturvaloukkaus havaittiin. (Andreasson & Ylipartanen 2022, 198.)

Epäillyn tietoturvaloukkauksen havaitsemisen jälkeen olisi hyvä tehdä tapauksesta riskiarvio. Jos tietoturvaloukkaus asettaa yksilön oikeudet ja vapaudet vaaraan, pitää rekisterinpitäjän ilmoittaa loukkauksesta tietosuojavaltuutetulle mahdollisimman pian ja viimeistään 72 tuntia loukkauksen havaitsemisesta. Lopullisen päätöksen ilmoittaa tietoturvaloukkauksesta myös rekisteröidyille tekee organisaation johto tai rekisterin vastuuhenkilö. Organisaation viestinnän vastuulla on laatia tietoturvaloukkauksesta kertova tiedote henkilöille, keitä tietoturvaloukkaus koskee. (Andreasson & Ylipartanen 2022, 199.)

Mikäli tietoturvaloukkauksessa epäillään tapahtuneen rikos, kuten tietomurto, loukkauksesta tehdään myös rikosilmoitus poliisille. Kalastelusta ja palvelunestohyökkäyksistä tehdään ilmoitus Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle. Lopuksi kun tarvittavat toimenpiteet on tehty tietoturvaloukkauksen korjaamiseksi ja selvittämiseksi käydään läpi dokumentaatiota ja varmistetaan, ettei organisaatiossa jatkossa toisteta samoja virheitä. Loukkaukset tulee myös tilastoida ja raportoida puolen vuoden välein ylimmälle johdolle. (Andreasson & Ylipartanen 2022, 199–200.)

2.6.2 Tietosuojavaltuutetun toimivaltuudet ja seuraamusmaksut

Yleisen tietosuoja-asetuksen mukaan jokaisella valvontaviranomaisella on oikeus tutkia rekisterinpitäjän tai henkilötietojen käsittelijän henkilötietojen käsittelyä tutkintavaltuuden nojalla. Tietosuojavaltuutetulla on oikeus muun muassa määrätä organisaatio antamaan valvontaviranomaiselle pääsy kaikkiin organisaation tehtävien suorittamiseen liittyviin tietoihin, toteuttaa tietosuojaan liittyviä tarkastuksia, ilmoittaa organisaatiolle yleisen tietosuoja-asetuksen väitetystä rikkomisesta ja saada pääsy organisaation tiloihin ja tietojenkäsittelylaitteille. Valvontaviranomaiset saavat myös tutkia sertifiointien paikkansa pitävyyttä ja rekistereiden suojaamiskäytäntöjä. (Andreasson & Ylipartanen 2022, 230–231.)

Yleinen tietosuoja-asetus antaa jokaiselle valvontaviranomaiselle hyväksymis- ja neuvontavaltuudet. Tietosuojavaltuutettu voi esimerkiksi antaa rekisterinpitäjälle neuvoja ennakkokuulemismenettelyssä, antaa henkilötietojen suojaan liittyviä neuvoja eduskunnalle, hallitukselle ja yleisölle omaaloitteisesti tai pyynnöstä, hyväksyä käytännesääntöjä, hyväksyä yritystä koskevia sääntöjä, myöntää sertifikaatteja, hyväksyä sertifiointikriteerejä sekä hyväksyä tiettyjä kansainvälisiin siirtoihin liittyviä sopimuslausekkeita. Tietosuojavaltuutetun toimisto toteuttaa tällä hetkellä neuvontavaltuuksia myös muun muassa julkaisemien päätöstensä ja ohjeistuksien kautta verkkosivuillansa. (Andreasson & Ylipartanen 2022, 231–232.)

Korjaavilla toimivaltuuksilla tarkoitetaan keinoja, joilla viranomainen pyrkii muokkaamaan organisaation henkilötietojen käsittelyä tietosuojalainsäädännön mukaiseksi. Tietosuojavaltuutettu voi korjaavana toimina esimerkiksi varoittaa rekisterinpitäjää kyseenalaisista aiotuista käsittelytoimista, antaa huomautuksen vääränlaisista käsittelytoimista, määrätä organisaatio noudattamaan rekisteröidyn pyyntöjä omien oikeuksiensa käyttöön liittyen, määrätä organisaatio ilmoittamaan tietoturvaloukkauksesta rekisteröidyille, asettaa väliaikainen tai pysyvä henkilötietojen käsittelykielto organisaatiolle, kumota tai määrätä sertifiointielimen peruuttamaan annetun sertifioinnin, määrätä hallinnollisen seuraamusmaksu seuraamuskollegion kautta sekä määrätä tiedonsiirron keskeyttämisestä kolmannessa maassa sijaitsevaan organisaatioon. Tietosuojavaltuutettu voi määrätä korjaavia toimenpiteitä kerralla yhden tai useamman. Tärkeää on, että toimit ovat tehokkaita ja varoittavat samalla muita organisaatioita toimimasta tietosuojasäädösten vastaisesti. (Andreasson & Ylipartanen 2022, 232–234.)

Suomessa tietosuojavaltuutettu ei saa suoraan itsenäisesti määrätä hallinnollisia seuraamusmaksuja, vaan siitä huolehtii seuraamuskollegio. Seuraamuskollegioon kuuluu tietosuojavaltuutettu sekä kaksi apulaistietosuojavaltuutettua, jotka yhdessä äänestävät korjaavien toimivaltuuksien käytöstä. Hallinnollisten seuraamusmaksujen ja sakkojen suuruuteen vaikuttavat muun muassa rikkomuksen kesto ja toistuvuus, rikkomuksen liiketoiminnallinen hyödynnettävyys, erityisiin

henkilötietoryhmiin kuuluvien tietojen käsittely ja hyödyntäminen, rekisteröityjen lukumäärä johon rikkomus vaikuttaa, rekisteröidyille aiheutuvien vahinkojen suuruus, rikkomuksen tahallisuus ja yhteistyö valvontaviranomaisen kanssa rikkomuksen korjaamiseksi ja lieventämiseksi. (Andreasson & Ylipartanen 2022, 240–244.)

3 Asiakastapahtumaa ja sen markkinointia koskevat tietosuojasäännöt

Markkinoinnilla tarkoitetaan yksinkertaistettuna kaikkea sellaista toimintaa ja viestintää, jolla pyritään myynninedistämiseen ja kuluttajan tai asiakkaan käyttäytymisen vaikuttamiseen. Markkinointi voi olla esimerkiksi sponsorointia, suoramarkkinointia ja digitaalista markkinointia. (ICC 2018, 8.) Asiakastapahtumilla voidaan pyrkiä pitämään vanhat asiakkaat jatkossakin organisaation asiakkaina tai luoda kokonaan uusia asiakassuhteita myynnin edistämiseksi. Asiakastapahtumat lasketaan markkinoinniksi, ja niitä koskevat markkinointiin liittyvien lakien ja sääntöjen lisäksi tietosuojasäädökset.

Asiakastapahtumien järjestämiseen liittyy tilanteita, joissa markkinoijan on hyvä tuntea mitä henkilötietoja asiakkaista saa kerätä, miten henkilötietoja saa käsitellä ja mitä tarkoituksia varten tietoja saa käyttää. Esimerkiksi tapahtumaa järjestettäessä on hyvä tietää miten asiakkaisiin saa olla yhteydessä ja mitä tietoja tapahtumaan osallistuvilta ihmisiltä on soveliasta pyytää. Asianmukainen tietojen kerääminen asiakkailta voi mahdollistaa esimerkiksi parempien tuotteiden kehittämisen ja paremmin kohdennettujen markkinointiviestien lähettämisen (Koivumäki 2022, 175).

Henkilötietojen käsittelyä koskevien lakien tarkoituksena on turvata ihmisten yksityisyyttä. Siksi markkinoinnin parissa työskentelevien on hyvä tunnistaa, milloin henkilötietojen käsittely on sallittua ja milloin ei. Henkilötietojen käsittelystä säädetään ja annetaan ohjeita markkinointiin liittyen muun muassa kuluttajansuojalaissa (38/1978) ja kansainvälisen kauppakamarin markkinointisäännöissä. (Koivumäki 2022, 175.)

3.1 Tapahtuman tietosuojaroolit, tietosuojaseloste ja tietojenkäsittelysopimus

Planmeca Oy:n tietosuojavastaavan mukaan silloin kun organisaatio järjestää tapahtuman yksin, on se vastuussa tapahtumaan osallistuvien asiakkaiden ja henkilöiden henkilötiedoista. Tämä tarkoittaa myös sitä, että ulkoistetut toimijat, eli tapahtumaa tukevat yritykset, ovat käsittelijöitä suhteessa organisaatioon, joka on rekisterinpitäjä. Rekisterinpitäjä on pääasiallisessa vastuussa tapahtumaan liittyvien henkilötietojen käsittelystä, joten sen täytyy sopia käsittelijöiden kanssa henkilötietojen käsittelystä tietojenkäsittelysopimuksella. Tyypillisiä henkilötietojen käsittelijöitä tapahtumissa ovat muun muassa catering-palvelut, viestintätoimistot, valokuvaajat, etäkokousjärjestelmät ja muut yritykset, joiden kanssa jaetaan henkilötietoja. Esimerkiksi catering-palvelujen kokeille voi joutua kertomaan erityisruokavaliota noudattavien ihmisten nimet, jolloin tietojenkäsittelysopimus on tehtävä.

Mikäli organisaatio järjestää tapahtuman yhteistyössä muiden yritysten kanssa ilman yhteisrekisterinpitäjyyttä, ovat kaikki yritykset itsenäisiä rekisterinpitäjiä. Tämä tarkoittaa sitä, että jokainen

tapahtumaan järjestämiseen osallistuva yritys määrittää itsenäisesti henkilötietojen käsittelyä koskevat sopimuksensa henkilötietoja käsittelevien yritysten, kuten valokuvaajien kanssa. Jokainen yritys joutuu myös pyytämään suostumusta erikseen henkilötietojen käsittelyä varten tapahtumaan osallistuvilta henkilöiltä.

Organisaation järjestäessä tapahtuman yhdessä yhden tai useamman yrityksen kanssa siten, että ne sopivat keskenään henkilötietojen käsittelyn tarkoitukset ja keinot, on kyseessä yhteisrekisterinpitäjyys. Tällöin yritykset yhdessä määrittelevät ja sopivat henkilötietojen käsittelyä koskevat seikat yhteiseen sopimukseen esimerkiksi henkilötietoja käsittelevien tukiyritysten ja asiakkailta kerättävien tietojen osalta. Yhteisrekisterinpitäjyydestä sovitaan kirjallisesti jokaisen rekisterinpitäjän, eli tapahtumaa järjestämässä olevan yrityksen kanssa. Yhteisrekisterinpitäjyys päättyy, kun henkilötietojen käsittelyn tarkoitus päättyy. (Korpisaari 2022, 326–327.)

Kaikilla yrityksillä, jotka keräävät työntekijöistään tai asiakkaistaan tietoja on tietosuojaselosteen laatimisvelvollisuus. Asiakastapahtumia järjestettäessä henkilötietojen keräämiseltä harvemmin voi välttyä, joten asiakastapahtuman järjestävän organisaation tulee laatia asianmukainen tietosuojaseloste. Tietosuojaselosteessa rekisteröidyille, eli asiakkaille kerrotaan mitä henkilötietoja heistä kerätään, miksi ja millaisin perustein. Yleisen tietosuoja-asetuksen artikloista 13 ja 14 pystyy johtamaan vaaditut tiedot tietosuojaselosteeseen. (Lindfelt 9.11.2022.) Tietosuojaselosteeseen tulee sisältyä ainakin seuraavat tiedot, ohjeet ja oikeudet:

- Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot;
- Tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot;
- Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;
- Jos käsittely perustuu oikeutettuun etuun, rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut;
- Kyseessä olevat henkilötietoryhmät;
- Henkilötietojen vastaanottajat tai vastaanottajaryhmät;
- Tiedot tietojen siirrosta kolmansiin maihin ja tiedot käytettävistä suojatoimista (sis. tiedon komission tietosuojan riittävyyttä koskevasta päätöksen olemassaolosta tai puuttumisesta) ja keinot saada kopio tai tieto niiden sisällöstä;
- Henkilötietojen säilyttämisaika tai, jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;
- Rekisteröidyn oikeudet (oikeus saada pääsy henkilötietoihin, oikeus tietojen oikaisemiseen oikeus tietojen poistamiseen, oikeus käsittelyn rajoittamiseen, vastustamisoikeus, oikeus siirtää tiedot järjestelmästä toiseen);
- Jos käsittely perustuu suostumukseen (tai nimenomaiseen suostumukseen), tieto oikeudesta peruuttaa suostumus milloin tahansa;

- Oikeus tehdä valitus valvontaviranomaiselle;
- Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus tai sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraamukset;
- Tiedot siitä, mistä henkilötiedot on saatu sekä tarvittaessa siitä, onko tiedot saatu yleisesti saatavilla olevista lähteistä; ja
- Tiedot automaattisen päätöksenteon, ml. profiloinnin olemassaolosta, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle. (Lindfelt 9.11.2022)

Yleisen tietosuoja-asetuksen artiklan 30 takia tietosuojaselosteeseen usein saatetaan laittaa, mikäli mahdollista myös kuvaus henkilötietojen käsittelyn teknisistä ja organisatorisista turvatoimista. Tietosuojaselosteen tulee olla tiivis, selkeä ja mahdollisimman helposti ymmärrettävällä kielellä kirjoitettu. Tietosuojaselosteita voi laatia erikseen erilaisia käyttötarkoituksia varten, esimerkiksi organisaation työntekijöille, tapahtumille ja asiakkaille on mahdollista laatia omat tietosuojaselosteensa. Tietosuojaselosteen tiedot täytyy toimittaa rekisteröidylle silloin kun häneltä kerätään tietoja, tai selosteen täytyy jollain muulla tavoin olla helposti saatavilla. Tietosuojaselosteeseen ohjaavan linkin voi laittaa näkyville muun muassa yrityksen kotisivuille, yhteydenotto-, tilaus- ja rekisteröintilomakkeisiin, uutiskirjeisiin, sähköpostimarkkinointiviesteihin tai rekisteröitymisten ja työhakemusten vastaanottamisviesteihin. (Lindfelt 9.11.2022.)

Markkinointikampanjoiden ja muidenkin tapahtumien toteuttamiseksi saatetaan käyttää apuna muita yrityksiä. Esimerkiksi suoramarkkinointikirjeiden postitus saatetaan ulkoistaa sitä tarjoavalle yhteistyökumppanille tai arpajaisten järjestäminen sen osaavalle mainostoimistolle. Näissä tapauksissa potentiaalisten asiakkaiden henkilötietoja käsittelee jokin muu toimija kuin rekisterinpitäjä. Yleisen tietosuoja-asetuksen mukaan vastaavanlaisissa tilanteissa rekisterinpitäjän tulee tehdä kirjallinen yhteistyösopimus, kuten tietojenkäsittelysopimus, yrityksen kanssa, joka käsittelee henkilötietoja sen lukuun. (Koivumäki 2022, 199.)

Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjä tulee käyttää henkilötietojen käsittelijöinä sellaisia yrityksiä, jotka huolehtivat osaltansa turvallisesta henkilötietojen käsittelystä. Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän apua ilman rekisterinpitäjän lupaa tai poiketa rekisterinpitäjän antamista ohjeista itsenäisesti. (Koivumäki 2022, 199.) Tietojenkäsittelysopimuksia voidaan tehdä myös itsenäisten rekisterinpitäjien ja yhteisrekisterinpitäjien välillä (Lindfelt 2025). Tietojenkäsittelysopimuksessa olisi hyvä olla vähintään seuraavia asioita sovittuna ja käsiteltynä:

1. Tietojen käsittelyn tarkoitus: Selitetään, mihin tarkoitukseen tietoja käsitellään.
2. Käsittelyn kesto ja luonne: Määritellään, kuinka kauan tietoja käsitellään ja millä tavalla niitä käsitellään.

3. Tietojen luovuttaminen: Sopimuksessa voidaan määritellä, saako käsittelijä luovuttaa tietoja kolmansille osapuolille tai toisille käsittelijöille.
4. Tietoturva: Sovitaan toimenpiteistä, joilla varmistetaan tietojen asianmukainen suojaaminen.
5. Käsittelijän velvollisuudet: Selvitetään, mitä velvollisuuksia käsittelijällä on tietojen käsittelyssä.
6. Rekisterinpitäjän velvollisuudet: Määritellään rekisterinpitäjän vastuut ja velvollisuudet tietojen luovutuksen yhteydessä.
7. Auditoinnit: Saattaa sisältää säännökset siitä, että rekisterinpitäjällä on oikeus tarkistaa käsittelijän tietoturvakäytännöt. (Lindfelt 2025.)

Tietojenkäsittelysopimusten käyttäminen on pakollista, mutta myös järkevää rekisterinpitäjän kannalta, koska se on aina lopullisessa vastuussa henkilötietojen lainmukaisesta käsittelystä. Tämän vuoksi tietojenkäsittelysopimuksessa kannattaa sopia henkilötietojen käsittelijän vahingonkorvallisuusvelvollisuudesta rekisterinpitäjälle, mikäli henkilötietojen käsittelijän toimista syntyisi vahinkoa rekisteröidyille. Rekisterinpitäjän kannalta on myös tärkeää, että henkilötietojen käsittelijä sitoutuu tietojenkäsittelysopimuksen myötä käsittelemään asiakastietoja huolellisesti ja tarkoituksenmukaisesti. (Koivumäki 2022, 200.)

3.2 Henkilötietojen kerääminen nykyisiltä ja potentiaalisilta asiakkailta

Yleisessä tietosuoja-asetuksessa ei ole tiettyjä säädöksiä koskien asiakkaita tai potentiaalisia asiakkaita, vaan asioita käsitellään yleisemmin pelkän rekisteröidyn kannalta. Siksi markkinoijan tulee arvioida tarkasti millä perustein potentiaalisen asiakkaan tiedot voi tallentaa asiakasrekisteriin ja millaista asiakasviestintää henkilöön voi kohdistaa. Asiakasrekisterissä on mahdollista käsitellä laajempia tietoja henkilöstä kuin potentiaalisten asiakkaiden suoramarkkinointirekisterissä. Pelkkä markkinointiarpajaisiin osallistuminen ei lähtökohtaisesti riitä perusteeksi henkilön tietojen talletta-miseen asiakasrekisteriin, vaan korkeintaan potentiaalisten asiakkaiden rekistereihin. (Koivumäki 2022, 194.)

Yleisessä tietosuoja-asetuksessa ei kerrota suoraan mitä kaikkia tietoja asiakasrekisteriin saa tallentaa. Siksi rekisterinpitäjän täytyykin noudattaa tietosuojaperiaatteita asiakastietojen keräämisessä ja kerätä heistä vain aidosti tarpeellisia ja asianmukaisia tietoja, jotka eivät turhaan supista rekisteröidyn yksityisyyden suojaa. Erityisen tarkkana kannattaa olla silloin kun organisaatio käyttää ulkoista toimijaa, kuten markkinointitoimistoa asiakkaiden tietojen keräämiseen. Tällöin mainostoimiston tulee tuntea organisaatio ja sen tietosuojaseloste hyvin kelle se kerää asiakkaista tietoja. Tämä johtuu siitä, ettei mainostoimisto vahingossa pyydä asiakkailta tarpeettomia tietoja, joiden keräämiseen organisaatiolla ei ole oikeutta. (Koivumäki 2022, 195.)

Asiakkaiden tietoja saa säilyttää asiakasrekisterissä niin kauan kuin rekisteröidyn ja organisaation välillä on olemassa jonkinlainen asianmukainen yhteys tai sopimussuhde, kuten kestosopimus. Asiakkaan ostaessa kertaluontoisesti jotain, henkilötietojen säilyttämisaika voi olla vaikea määritellä. Asianmukaisen yhteyden jälkeen rekisteröidyn tietoja saa kuitenkin käsitellä asiakasrekisterissä vielä kohtuullisen ajan verran. Tämä mahdollistaa edelleen joksikin aikaa asiakasviestinnän ja suoramarkkinoinnin henkilölle. (Koivumäki 2022, 195.)

Suomessa asianmukaisen yhteyden päättymisen jälkeen kohtuullisena pidettyä henkilötietojen säilytysaikana on pidetty jopa 3–4 vuotta. Erityislainsäädäntö saattaa vaikuttaa asianmukaisen yhteyden kestoon. Siksi esimerkiksi perinnän ja takuun voimassaolon ajan asianmukainen yhteys jatkuu ja tietojen säilyttäminen voi olla mahdollista pitkäänkin. Kohtuullisen ajan jälkeen rekisteröidyn kaikki tiedot tulee poistaa asiakasrekisteristä tai siirtää sallitut tiedot pysyvään suoramarkkinointirekisteriin. (Koivumäki 2022, 195.)

Yleisen tietosuoja-asetuksen mukaan oikeutettu etu sopii alustavaksi perusteeksi potentiaalisten asiakkaiden suoramarkkinointirekisterien ylläpitämiselle. Suoramarkkinointirekistereihin voi kerätä tietoja myös rekisteröidyn suostumukseen perustuen tai muulla laillisella tavalla. B2B -markkinointirekistereihin voi kerätä tietoja, jotka ovat olennaisia käyttötarkoitustaan varten. Kerättävien tietojen tulisi koskea esimerkiksi potentiaalisen yritysasiakkaan yhteyshenkilön asemaa, yhteystietoja ja muita henkilön työhön liittyviä tehtäviä. (Koivumäki 2022, 196.)

3.3 Suoramarkkinoinnin ja asiakasviestinnän tietosuoja

Suoramarkkinoinnilla tarkoitetaan markkinointia, joka on suunnattu tietylle henkilölle käyttäen tämän tavoittamiseen hänen yhteystietojaan, kuten esimerkiksi postiosoitetta, sähköpostiosoitetta, puhelinnumeroa tai some-tiliä (ICC 2018, 29). Perinteisellä suoramarkkinoinnilla tarkoitetaan puhelimitse tai postitse tapahtuvaa markkinointia (Koivumäki 2022, 201). Sähköisellä suoramarkkinoinnilla tarkoitetaan markkinointia, joka tapahtuu sähköisesti. Sähköiseksi suoramarkkinoinniksi katsotaan automatisoitujen soittojärjestelmien, faxien, sähköpostiviestien, tekstiviestien, puheviestien, ääniviestien tai kuvaviestien avulla toteutettu suoramarkkinointi. (Koivumäki 2022, 204.)

Sähköisen viestinnän palveluja koskevan lain mukaan sähköinen suoramarkkinointiviesti tulee olla helposti tunnistettavissa markkinoinniksi. Sellaisten markkinointiviestien lähettäminen on kiellettyä, joissa peitetään tai salataan viestin lähettäjän henkilöllisyys, jossa ei ole voimassa olevaa osoitetta markkinointiviestien lähettämisen lopettamiseen tai markkinointiviestin vastaanottaja pyritään ohjaamaan sopimattomille tai epäilyttäville verkkosivuille. (Koivumäki 2022, 216.)

Markkinointiviesteihin täytyy myös muistaa laittaa mukaan tietosuojainformaatio esimerkiksi linkin muodossa sekä kertoa viestin vastaanottajalle kielto-oikeudesta. Sähköposteihin voi laittaa

esimerkiksi ”klikkaa tästä, jos et halua jatkossa vastaanottaa viestejämme” -linkin. Tekstiviesteissä kielto-oikeudesta voi kertoa esimerkiksi ”Kiellot: 0800 xxxx” tekstillä viestin lopussa. Puhelimitse tehtävästä peruutuksesta ei saa periä erillistä maksua, joten rekisteröity maksaa perumisesta vain normaalihintaisen puhelun verran. (Koivumäki 2022, 216.)

3.3.1 Perinteinen ja sähköinen suoramarkkinointi kuluttajalle

Kuluttajalle saa tehdä markkinointia perinteisillä menetelmillä vapaasti ilman ennakkosuostumusta Kuluttaja voi kuitenkin halutessaan kieltää markkinoinnin ja hänelle tulee kertoa kielto-oikeudesta asiakassuhteen tai muun yhteydenpidon aloitushetkellä. Kielto-oikeudesta voi kertoa esimerkiksi organisaation tietosuojaselosteen avulla. Organisaation on myös informoitava asiakasta, jos se aikoo kohdistaa häneen perinteistä suoramarkkinointia esimerkiksi arvonnan yhteydessä kerättyjen yhteystietojen avulla. Suomessa kuluttajalle tehtävään perinteiseen suoramarkkinointiin liittyvää toimintatapaa kutsutaan opt out -menettelyksi. Perinteistä suoramarkkinointia harjoittaessa organisaation tulee huolehtia, että sen käsittelemät yhteystiedot on saatu laillisin keinoin ja sillä on riittävät perusteet henkilötietojen käsittelyyn. (Koivumäki 2022, 201–202.)

Puhelimessa tapahtuvan suoramarkkinoinnin sääntelyyn tuli vuoden 2023 alussa muutos, joka velvoittaa puhelinmarkkinoijan lähettämään kirjallisen tarjouksen kuluttajalle myyntipuhelun päätyttyä. Kirjallinen tarjous voi olla esimerkiksi tekstiviesti, johon vastaamalla kuluttaja hyväksyy tarjouksen. Menettelyä kutsutaan niin sanotusti puhelinmyynnin jälkivahvistukseksi. Mikäli asiakas on itse yhteydessä yritykseen tai on jättänyt yhteydenottopyynnön yritykselle, ei jälkivahvistusta tarvita. (Koivumäki 2022, 202–204.)

Markkinointipuheluja saa nauhoittaa puhelun sisällön todentamiseksi sekä koulutustarkoitusta tai laadun tarkkailua varten. Asiakkaalle tulee kertoa nauhoittamisesta mahdollisimman pian puhelun alettua. Nauhoitettua puhelua ei saa tuoda esille julkisesti, ellei siitä ole sovittu asiakkaan kanssa. Mikäli kuluttajan puhelinnumero on salainen, hänelle ei saa soittaa markkinointipuheluja, paitsi jos hän on itse antanut numeronsa yritykselle. (ICC 2018, 35.)

Suomessa sähköisessä suoramarkkinoinnissa on käytössä niin sanottu opt in -menettely. Kuluttajalle ja potentiaaliselle asiakkaalle saa tehdä sähköisiä viestimiä hyödyntäen tarjouksia, vain silloin kun hän on antanut siihen etukäteen suostumuksensa. Suostumuksen tulee olla vapaaehtoisesti annettu ja kuluttajan tulee itse esimerkiksi rastittaa verkkolomakkeen suostumuskohta, jossa hän luovuttaa yhteystietonsa sähköistä suoramarkkinointia varten. Viranomaislinjausten mukaan verkkolomakkeissa ei ole suositeltavaa käyttää lupapyyntöjen kohdalla valmiiksi rastitettuja suostumuksia, joista kuluttajan täytyisi poistaa rasti, jos hän ei halua antaa yhteystietojansa sähköistä suoramarkkinointia varten. Lupapyyntöjä varten kuluttajalle pitää antaa myös tarpeeksi informaatiota

käsittelyn tarkoituksista, jotta hän voi arvioida mihin on suostumassa. Tilanteissa, joissa jokin tuote tilataan lahjaksi, ei voida katsoa lahjansaajan antaneen suostumusta sähköistä suoramarkkinointia varten. (Koivumäki 2022, 205–206.)

Sähköisen suoramarkkinoinnin lupapyyntöjen sisältöjä kannattaa pohtia huolellisesti. Lupaa voidaan pyytää moneenkin asiaan samaan aikaan ja esimerkiksi kuluttajalta on mahdollista kysyä, sopiiko hänelle sähköisen suoramarkkinoinnin lähettäminen sähköpostitse ja sms- tai mms-viestein. On kuitenkin hyvä pohtia voiko laajat pyynnöt vähentää kuluttajien lupien antamista sähköiseen suoramarkkinointiin. Lisäksi EU:n tietosuojaviranomaisten mukaan sähköisen suoramarkkinoinnin tavoista olisi jokaisesta hyvä pyytää erikseen lupaa. Eli esimerkiksi sähköpostin lähettämisestä ja tekstiviestin lähettämisestä tulisi kysyä lupa kahdella erillisellä kysymyksellä. (Koivumäki 2022, 209–210.)

Lupapyyntöjen sisältöjä ei kuitenkaan kannata muotoilla kovin tarkkarajaiseksi. Tämä johtuu siitä, että organisaation liiketoiminnan ja markkinoinnin muodot saattavat muuttua toisenlaisiksi, jolloin voi esimerkiksi tulla tarve olla kuluttajaan useammin yhteydessä kuin lupapyynnössä oli yksilöity. Lupaa sähköiseen suoramarkkinointiin voidaan kysyä organisaation omaa markkinointia, samaan konserniin kuuluvia yhtiöitä tai organisaation yhteistyökumppaneita varten. Yhteistyökumppaneiden nimet olisi hyvä kertoa lupapyynnössä kuluttajalle. (Koivumäki 2022, 210.)

Lupapyynnössä tulisi antaa tietoa siitä, kuinka usein ja minkä tyyppistä suoramarkkinointia kuluttaja tulee saamaan suostuessaan antamaan yhteystietonsa sähköistä suoramarkkinointia varten. Kuluttajalle olisi esimerkiksi hyvä kertoa tuleeko hän saamaan viikkokirjeitä vai kuukausikirjeitä ja saako hän esimerkiksi tietoa uutuustuotteista, eduista, tarjouksista vai kutsuista. Kuluttajalla on milloin tahansa oikeus peruuttaa antamansa suostumus sähköiseen suoramarkkinointiin liittyen. (Koivumäki 2022, 210.)

Lupapyyntöjä suoramarkkinointiin ei kuitenkaan tarvita sellaisessa poikkeustapauksessa, jossa sähköistä suoramarkkinointia kohdistetaan organisaation olemassa oleville asiakkaille. Sähköisen viestinnän palveluita koskevan lain mukaan palvelun tarjoaja tai tuotteen myyjä saa lähettää asiakkaalle sähköistä suoramarkkinointia omista samaan tuoteryhmään kuuluvista palveluista tai tuotteista esimerkiksi sähköpostitse tai tekstiviestinä, mikäli palvelun tarjoaja tai tuotteen myyjä on saanut asiakkaan yhteystiedon palvelun tai tuotteen myynnin yhteydessä. Palvelun tarjoajan tai tuotteen myyjän on kuitenkin tarjottava asiakkaalle mahdollisuutta kieltäytyä suoramarkkinoinnista maksutta jokaisen markkinointiviestin, kuten sähköpostiviestin yhteydessä. Sähköisestä suoramarkkinoinnista kieltäytymisen tulee olla helppoa ja siitä tulee tiedottaa mahdollisimman selkeästi. (Koivumäki 2022, 210.)

Sähköistä suoramarkkinointia saa lähettää kuluttajalle vain se yritys, kenelle kuluttaja on antanut oston yhteydessä yhteystietojansa. Tämä tarkoittaa konsernien osalta sitä, että vain se osakeyhtiö kuka on solminut asiakkaan kanssa kaupan, voi ainoastaan hyödyntää asiakkaan yhteystietoja suoramarkkinoinnissa. Myynnin ja yhteystietojen luovuttamisen yhteydessä kuluttajalle täytyy myös muistaa kertoa, että hän tulee saamaan sähköistä suoramarkkinointia esimerkiksi sähköpostiinsa ja puhelimeensa, ja että hän voi kieltäytyä suoramarkkinoinnista koska tahansa. Kaupanteon yhteydessä annetulla huolellisesti suunnitellulla tietosuojainformaatiolla mahdollistetaan monipuolinen suoramarkkinointivalikoima. (Koivumäki 2022, 212.)

3.3.2 Perinteinen ja sähköinen suoramarkkinointi business to business -toiminnassa

Perinteisen suoramarkkinoinnin osalta business to business -toiminnassa on Suomessa käytössä niin sanottu opt out -menettely. Yritysten yhteyshenkilöille saa soittaa markkinointipuheluja ja yrityksille saa lähettää postitse suoramarkkinointia ilman ennakkosuostumusta. Perinteinen suoramarkkinointi tulee kuitenkin lopettaa, mikäli vastaanottaja kieltää sen. Kielto-oikeudesta on annettava tietoa esimerkiksi rekisteriselosteessa, asiakassuhteen alussa tai muun yhteydenpidon aloitushetkellä. (Koivumäki 2022, 212–213.)

Sähköisen suoramarkkinoinnin osalta business to business -toiminnassa on Suomessa käytössä niin sanottu opt out -menettely. Yritysten ja yhteisöjen yhteyshenkilöille saa lähettää heidän tehtäväänsä liittyvää suoramarkkinointia ilman ennakkosuostumusta esimerkiksi sähköpostitse. Sähköinen suoramarkkinointi tulee kuitenkin pystyä lopettamaan ja kieltämään veloituksetta, mikäli vastaanottaja haluaa lakata saamasta suoramarkkinointia. Kielto-oikeudesta on annettava tietoa esimerkiksi rekisteriselosteessa, asiakassuhteen alussa tai muun yhteydenpidon aloitushetkellä. (Koivumäki 2022, 213.)

Yritykselle voi lähettää sen toimintaan liittyvää sähköistä suoramarkkinointia, myös silloin kun yritys on antanut siihen luvan esimerkiksi uutiskirjetilauksen kautta. Myös voimassa oleva asiakkuus antaa mahdollisuuden lähettää sähköistä suoramarkkinointia yritykselle. Yrityksille ei saa lähettää kuluttajille suunnattua markkinointia, vaan suoramarkkinointiviestin sisällön pitää olla kohderyhmälle sopiva. (Koivumäki 2022, 213–215.)

3.3.3 Suoramarkkinoinnin ja asiakasviestinnän ero

Suoramarkkinointia ja asiakasviestintää koskevat erilaiset säädökset. Asiakkaalla ei ole laillista oikeutta kieltäytyä häntä koskevasta asiakasviestinnästä. Organisaatio saa myös itse valita mitä tapaa, kuten esimerkiksi sähköpostia ja tekstiviestiä, se käyttää asiakasviestinnässään. Ero suoramarkkinoinnin ja asiakasviestinnän välillä ei aina ole kuitenkaan selkeää, joten asiakasviestintää suunniteltaessa pitää olla tarkkana sen sisällöstä. (Koivumäki 2022, 220.)

Asiakasviestintänä pidetään viestintää, jonka tarkoituksena on asiakassuhteen hoitamiseksi tarvittava yhteydenpito, mihin ei liity markkinointia. Asiakasviestinnässä asiakas saa tietoja valitsemansa palvelun tilanteesta, jatkuvuudesta tai muuttumisesta. Esimerkiksi, kun autokorjaamo lähettää asiakkaalleen viestin auton olevan valmis noudettavaksi ilman mainoksia, niin on kyse asiakasviestinnästä. (Koivumäki 2022, 221.)

Organisaatio saa lähettää asiakkailleen ja jäsenilleen asiakasviestintää uutiskirjeinä, kunhan ne eivät sisällä mainoksia. Suoramarkkinointia sisältävän uutiskirjeen lähettämiseen vaaditaan kuitenkin vastaanottajalta lupa. Mikäli kuluttajalle lähetetään asiakasviestintää sähköisesti, kuten sähköpostitse, tulee viestin lähettäjän voida perustella viestinnän tarve esimerkiksi tietyllä lainkohdalla. Tietosuojasäädösten mukaan kuluttajaa on myös informoitava henkilötietojen käsittelyn tarkoituksista. Siksi mahdollisesta sähköisestä asiakasviestinnästä, kuten uutiskirjeiden lähettämisestä, olisi suositeltavaa informoida kuluttajaa jo henkilötietoja kerättäessä, vaikka lainsäädännön puitteissa sitä ei vaadita. Selkeä informointi organisaation viestintäkäytännöistä kasvattaa asiakkaiden luottamusta organisaatiota kohtaan. (Koivumäki 2022, 221–224.)

3.3.4 Asiakastapahtuman suoramarkkinointi ja asiakasviestintä

Planmeca Oy:n tietosuojavastaavan mukaan asiakastapahtuman markkinointia koskevat samat säännöt kuin suoramarkkinointia ja asiakasviestintää. Kuluttajille tapahtumakutsun lähettäminen kirjeitse tai siitä puhelimitse tiedottaminen on sallittua ilman ennakkosuostumusta. Sähköpostimarkkinointi edellyttää ennakkosuostumuksen, ja kuluttajalla on oikeus tarvittaessa saada tietää mistä hänen yhteystietonsa on peräisin. Tapahtumakutsun hyväksyminen puhelimessa edellyttää kuluttajalta kirjallista jälkivahvistusta soiton jälkeen.

Jälkivahvistus tarkoittaa sitä, että kutsu tai tarjous pitää olla tallennettavissa tai kopioitavissa. Kuluttajalle on myös ilmoitettava, ettei tule sidotuksi sopimukseen, jos ei hyväksy sitä pysyvällä tavalla. Jos kuluttaja ottaa yhteyttä yritykseen omasta aloitteestaan, kirjallista vahvistusta ei vaadita. Mikäli kuluttajalla on voimassa markkinointikielto, kuluttajalle ei saa soittaa tai laittaa sähköpostia tapahtumista tai tarjouksista.

Yrityksille tapahtumakutsun lähettäminen kirjeitse tai sähköpostitse on sallittua ilman ennakkosuostumusta. Myös puhelinmarkkinointi tapahtumasta on sallittua. Yrityksille kannattaa lähettää puhelimessa sovitusta tapahtumaan osallistumisesta esimerkiksi linkki sähköpostiin, jossa yritys voi käydä vahvistamassa osallistumisensa.

3.3.5 Kiinnostuksen mukaista mainontaa (IBA) koskevat säännöt

IBA (Interest-Based Advertising) tarkoittaa internetin käyttäjän nettikäyttäytymisestä kerättyjen tietojen hyödyntämistä henkilölle kohdennetussa mainonnassa toisiinsa liittymättömillä verkkosivuilla tai sovelluksissa. Nettikäyttäytyminen voi olla esimerkiksi tiettyjen tuotteiden selaamista verkkokaupassa tai hakukoneen käyttämistä. Nettikäyttäytymisestä pystytään muodostamaan segmenttejä, joiden avulla kolmas osapuoli pystyy määrittelemään tietyille henkilöille soveltuvimmat mainokset. Kohdennettuja mainoksia voi nähdä esimerkiksi sosiaalisessa mediassa tai erilaisilla verkkosivuilla. (ICC 2018, 36.)

IBA-mainontaa hyödyntävien osapuolien on tärkeää olla avoimia kuluttajan tietojen keräämisestä ja kohdennettujen mainosten käyttämisestä. Kolmannen osapuolen ja verkko-operaattorin täytyy ilmoittaa verkkosivuillaan selkeästi IBA-mainontaan liittyvät omat käytännöt sekä kuvaukset tiedoista, joita kerätään sekä tiedonkeräämisen tarkoitukset. Verkkosivuilla tulee myös olla näkyvissä yhdellä tai useammalla tavalla tieto siitä, kuinka kuluttaja voi käyttää valinnanvapauttaan tietojen keräämisestä IBA-tarkoituksia varten. IBA-tarkoituksista voi ilmoittaa esimerkiksi mainoksen lähellä olevalla kuvakkeella, jonka linkki vie sivulle, jossa kerrotaan tietojen keräämisestä ja kolmansista osapuolista. Kolmannen osapuolen tulee antaa käyttäjälle mahdollisuus päättää, saako hänen tietojansa kerätä IBA-mainonnan kohdistamista varten. (ICC 2018, 36.)

IBA-mainontaa varten voidaan kerätä laitteen sijaintitietoja. Sijaintitiedot on mahdollista saada esimerkiksi GPS-pohjaisten leveys- tai pituuspiirikoordinaattien tai paikkaperusteisen taajuussignaalin kolmiomittauksen avulla. Tarkka sijaintitieto ei sisällä postinumeroa tai kaupunkia, vaikka sijaintitieto olisi saatu IP-osoitteesta tai muista lähteistä. Yksityisyyttä koskevien ilmoitusten täytyy kuitenkin kertoa mitkä verkkosivut, sovellukset ja palvelut saavat haltuunsa tarkkoja maantieteellisiä sijaintitietoja, ja kuinka ne käyttävät tai jakavat näitä tietoja. Yritysten tulee myös kertoa kaikista tavoista, miten sijaintitietoja kerätään. Sijaintitietoja voidaan esimerkiksi kerätä wifin tai langattoman lähiverkon verkkotunnuksen avulla. Reaaliaikaista mainosta varten kerättyjä tarkkoja sijaintitietoja saa säilyttää vain keräämishetkellä tarkoitettua yksilöityä käyttötarkoitusta varten. (ICC 2018, 36–37.)

Verkkosivustojen ja sovellusten tulee kertoa kuluttajalle ja ensimmäiselle osapuolelle kaikista tavoista, joilla ne harjoittavat laitteiden välistä seurantaa. Laitteiden välistä seurantaa voidaan toteuttaa esimerkiksi evästeiden, laitteiston tunnistamisen (fingerprinting) ja evästeiden synkronoinnin avulla. Mikäli kuluttaja kieltää IBA-mainonnan yhdellä laitteella, tämä kielto koskee myös muita laitteita, jotka ovat yhteydessä laitteeseen, jolla kielto tehtiin. Jos kaikista yrityksen IBA-mainontaan liittyvistä seurantatavoista ei voi kieltäytyä, tästä pitää ilmoittaa kuluttajalle selkeästi. (ICC 2018, 37.)

Kerättäessä arkaluontoisia tietoja IBA-segmenttejä varten, on verkkokäyttäjältä saatava erikseen suostumus tietojen käyttämisestä IBA-mainonnassa. Jos IBA-mainontaa varten luodaan lapsisegmenttejä, tähän vaaditaan vanhemman lupa. IBA-mainontaa varten kerättyjä tietoja saa säilyttää vain niin kauan kuin se on tarpeen liiketoiminnassa. Tietojen turvaamiseksi yrityksen täytyy myös huolehtia fyysisistä, elektronisista ja hallinnollisista turvajärjestelyistä. (ICC 2018, 37.)

3.3.6 Profilointi

EU:n yleisen tietosuoja-asetuksen mukaan profilointi tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä, jossa arvioidaan ja ennakoidaan luonnollisen henkilön henkilökohtaisia piirteitä liittyen työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin. Profilointi voi pohjautua muun muassa asiakkuudesta kerääntyneeseen tietoon, evästeiden avulla nettikäyttäytymisestä saatavaan tietoon tai henkilö on voinut itse suoraan kertoa mistä on kiinnostunut ja esimerkiksi ilmaissut haluavansa saada mielenkiinnonkohteestaan suoramarkkinointia. (Kuusimaa 1.3.2017.) Yksinkertainen ikään, sukupuoleen ja pituuteen perustuva henkilöiden luokittelu ei lähtökohtaisesti ole profilointia, jos tiedot on kerätty tilastointia varten, ja tiedoista ei pyritä tekemään henkilökohtaisia arvioita markkinoinnin kohdentamiseksi (Koivumäki 2022, 218).

Profiloinniksi ei katsota tilannetta, jossa ihminen, kuten lainanantaja, tekee yleisen elämänkokemuksensa perusteella arvion, miten toinen henkilö tulee käyttäytymään. Mikäli lainantaja käyttää arviossaan hyödyksi tietokonetta ja algoritmeja, niin silloin kyse on profiloinnista. Profilointia hyödynnetään myös internetin kohdennetuissa mainoksissa, jossa pyritään esimerkiksi evästeiden avulla tavoittamaan potentiaalisimmat asiakkaat. (Kuusimaa 1.3.2017.)

Yleisen tietosuoja-asetuksen mukaan henkilöllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi, kuten profiloinnin, jolla on häneen kohdistuvia oikeusvaikutuksia tai joka muuten vaikuttaa häneen vastaavalla tavalla. Taloudelliset vaikutukset voidaan katsoa oikeusvaikutuksia vastaaviksi vaikutuksiksi. Tämä tarkoittaisi sitä, että jos kahdelle eri asiakkaalle tarjottaisiin profilointia hyödyntäen samasta julkisesti hinnoitellusta tuotteesta eri hintaa, niin tulisi miettiä voiko tällaista suosimista edes tehdä, ja millä perustein. Hintasyrjinnästä puhutaan silloin kun eri ostajilta pyydetään samasta tuotteesta tai palvelusta eri hintaa, vaikka syrjimiselle ei ole mitään perusteita. Jonkun toisen asiakkaan positiivista suosimista voi tehdä vain silloin, kun se tehdään esimerkiksi kokonaisasiakkuuden ja hyvien asiakassuhteiden säilyttämisen perusteella. (Kuusimaa 1.3.2017.)

Profilointi on lähtökohtaisesti sallittua markkinoinnissa ilman henkilöltä erikseen saatua suostumusta. Henkilöllä on kuitenkin mahdollisuus vastustaa milloin tahansa hänen henkilötietojensa käsittelyä suoramarkkinointia varten, mikä kattaa siis profiloinnin, jos sitä hyödynnetään

markkinoinnissa. Vastustusoikeudesta tulee kertoa henkilölle suoramarkkinoinnin yhteydessä. (Kuusimaa 1.3.2017.)

Markkinointiin liittyvällä profiloinnilla on harvemmin kovin dramaattisia vaikutuksia kohderyhmänsä elämään, kun se on tehty huolellisesti. Lisäksi markkinoijalla on oikeus itsenäisesti arvioida kenen se luulisi olevan kiinnostunut sen palveluista ja tarjota niitä heille itse määrittelemillään ehdoilla, kunhan se ei syyllisty syrjintään. Profilointia saa käyttää myös, jos se on välttämätöntä sopimuksen tekemistä tai täytäntöönpanoa varten, rekisteröidyn oikeuksien ja vapauksien suojaamiseksi tai rekisteröity on antanut profiloinnille nimenomaisen suostumuksensa. (Kuusimaa 1.3.2017.)

3.4 Valo- ja videokuvauksen, webinaarien, osallistujalistojen ja käyntikorttien tietosuoja tapahtumissa

Valo- ja videokuva lasketaan yleisen tietosuoja-asetuksen mukaisesti henkilötiedoksi, jos siinä esiintyvä henkilö tai henkilöt ovat selvästi tunnistettavissa. Tällaisten valo- ja videokuvien käyttämiseen esimerkiksi markkinointitarkoituksiin tulisi kysyä lupa kuvan kohteelta. Lupaa voidaan kysyä esimerkiksi ilmoittautumisen yhteydessä, jolloin valokuvaajaa varten olisi hyvä erotella henkilöt ketkä suostuvat kuvattavaksi. Vapaaehtoinen asettautuminen kuvattavaksi tapahtumaan rakennetun kuvausseinän eteen, käy suostumukseksi siihen, että kuva voidaan julkaista. Erillistä kirjallista suostumusta ei tarvita, mutta tällaistakaan kuvaa ei saa käyttää mainoksessa ilman henkilön suostumusta. Mikäli tapahtumasta otetusta yleiskuvasta ei pysty tunnistamaan erityisesti ketään henkilöä, saa kuvan esimerkiksi jakaa sosiaalisessa mediassa, ilman etukäteen kysyttyä lupaa. (Halsvaha 27.5.2024, 21:30-23:00 min.)

Julkisilla paikoilla, kuten kaduilla, toreilla, metsissä tai muissa yleisölle julkisissa tiloissa dronella kuvaaminen on sallittua. Toisen henkilön asunnon tai sen ikkunan edessä kuvaaminen on kiellettyä, koska se rikkoo asukkaan kotirauhaa ja yksityisyyttä. Dronea ei saa lennättää valtiolle kuuluvien tärkeiden kohteiden kuten voimalaitosten, armeijan ja ydinvoimaloiden lähettyvillä. Traficomin ylläpitämältä droneinfo-sivulta on mahdollista tarkistaa alueet, joilla dronen lennättäminen on kiellettyä. (Andreasson ym. 2023, 221.)

Webinaaria tai muuta etätapahtumaa järjestettäessä on mietittävä etukäteen mitä yksityisyyteen liittyviä tietokoneen asetuksia hyödynnetään, tallennetaanko webinaari ja mitä tallenteelle tehdään. Webinaaria varten kerätään usein siihen osallistuvien henkilöiden nimet, sähköpostiosoitteet ja joskus jopa sijaintitiedot. Näiden tietojen käsittelyä ja säilyttämistä varten tarvitaan jokin peruste, kuten webinaariin osallistuvan henkilön suostumus tai muu peruste. Webinaariin osallistuvia henkilöitä on myös informoitava, mikäli heidän tietojaan näkyy webinaarin aikana muille osallistujille tai tilaisuudesta otetulla tallenteella. Webinaarin teknisenä alustana kannattaa käyttää yleisesti

tunnetun yrityksen webinaarin pitämiseen tarkoitettuja sovelluksia, koska henkilötietoja jaetaan sovelluksen kautta niin sanotusti kolmannelle osapuolelle. (Dixit 18.11.2024.)

Yleinen väärinkäsitys on, että henkilötietojen, kuten nimen, yhteystietojen tai ammattinimikkeen jakamiseen tarvittaisiin aina suostumus. Tapahtumanjärjestäjä voi käyttää suostumuksen lisäksi henkilötietojen jakamisen perusteena esimerkiksi oikeutettua etua osallistujalistojen laatimiseen ja nimikylttien käyttämiseen, mikäli tapahtuman luonne vaatii sen onnistuakseen. Oikeutettua etua voi käyttää henkilötietojen käsittelyn ja jakamisen perusteena silloin, kun tapahtumanjärjestäjän etu ei ole tärkeämpi kuin osallistujien edut tai oikeudet. Verkostoitumistapahtumien kaltaisissa tapahtumissa osallistujat voivat hyvinkin odottaa, että heille jaetaan osallistujalistoja ja nimikylttejä verkostoitumista varten. Tällöin oikeutettu etu sopii hyvin perusteeksi henkilötietojen käyttämisessä osallistujalistoissa ja nimikylteissä. Ennen tapahtumaa on kuitenkin hyvä kertoa siihen osallistuville henkilöille ilmoittautumisen yhteydessä, miten heidän tietojaan aiotaan käyttää ja antaa heille mahdollisuus esimerkiksi kieltäytyä nimikylttien käytöstä, jos he eivät halua heidän tietojaan muiden näkyviin. (Data Protection Commission Ireland 28.2.2020.)

Kun tapahtumaan osallistuja itse antaa käyntikorttinsa, niin tämä tulkitaan suostumukseksi henkilötietojen, eli kortissa olevien tietojen käsittelyyn ja säilyttämiseen. Kortin tietojen avulla saa olla sen antaneeseen henkilöön yhteydessä perinteisen tai sähköisen suoramarkkinoinnin keinoin riippuen onko kortin antanut henkilö tavallinen kuluttaja vai yrityksen edustaja. Yrityksen edustajalle saa lähettää sähköpostitse suoramarkkinointia kortin tietoja käyttäen, mutta tavalliselta kuluttajalta sähköiseen suoramarkkinointiin täytyy pyytää erikseen lupa. (Siney 8.6.2018.)

3.5 Sosiaalisen median, arvontojen ja kilpailujen tietosuoja

Sosiaalinen media on käytössä lähes kaikilla ja siksi siellä on hyvä jakaa tietoa vaikkapa yrityksen uusista tapahtumista, tuotteista tai kuulumisista. Suosittuja sosiaalisen median kanavia ovat esimerkiksi WhatsApp, YouTube, Facebook, Instagram, LinkedIn ja TikTok. Näissä kaikissa palveluissa käsitellään käyttäjien henkilötietoja, mutta jokainen käyttäjä voi itse määritellä kuinka paljon ja millä tavoin hän haluaa jakaa tietoja tai kuvia itsestään sosiaalisen median alustalle. (Andreasson ym. 2023, 139–142.)

Sosiaalisen median palvelujen tietosuojaan liittyvissä säännöissä saattaa olla paljon eroja ja niiden tietosuojainformaatiot voivat olla hankalasti löydettävissä. Yrityksen käyttäessä sosiaalista mediaa, sille muodostuu yhteisrekisterinpitäjyys sosiaalisen median palveluntarjoajan, kuten Facebookin kanssa. Yhteisrekisterinpitäjyys syntyy silloin kun yrityksen julkaisut keräävät tykkäyksiä ja yrityksen omalle somekanavalle kerääntyy seuraajia. (Väyrynen 3.2.2022, 9-10min.) Julkaistaessa yrityksen omille somekanaville videoita ja kuvia juhlista tai tapahtumista on hyvä kysyä niissä

esiintyviltä henkilöiltä hyväksyntä heidän näkymisestään somejulkaisuissa (Väyrynen 3.2.2022, 13-14min).

Kerättäessä henkilötietoja somen kautta, pitää miettiä millä perustein tietoja kerätään. Silloin kun asiakassuhdetta ei vielä ole, niin oikeutettua etua voi olla mahdollista käyttää perusteena tietojen keräämiseen. Somen kautta kerätessä tietoja, pitää huolehtia kaikkien tietosuojaperiaatteiden toteutumisesta, kuten rekisteröidyn oikeuksista, tietojen minimoinnista ja tietosuojainformaation antamisesta rekisteröidyille. (Väyrynen 3.2.2022, 17:30-20:50min)

3.5.1 Arvonnat ja kilpailut

Arvontojen ja kilpailujen yhteydessä yleensä kerätään rekisteröityjen yhteystietoja. Rekisterinpitäjä saa kerätä vain sellaisia henkilötietoja, jotka ovat oikeasti tarpeellisia kilpailun tai arvonnan suorittamiseksi. Kerättäessä henkilötietoja, rekisteröityä tulee informoida muun muassa siitä mihin tarkoitukseen tietoja tullaan käyttämään ja kuinka kauan tietoja säilytetään. (Tietosuojavaltuutetun toimisto 2025a.)

Mikäli kerättyjä henkilötietoja aiotaan käyttää sähköiseen suoramarkkinointiin, tähän täytyy kysyä erikseen lupa rekisteröidyltä. Rekisteröidyltä voi kysyä lupaa sähköiseen suoramarkkinointiin esimerkiksi pyytämällä häntä rastittamaan ruudun, jossa hän ilmaisee halunsa saada markkinointimateriaalia arvonnan tai kilpailun järjestävältä organisaatiolta. Jos lupaa sähköiseen suoramarkkinointiin ei saada, voi rekisteröityyn olla yhteydessä vain arvontaan tai kilpailuun liittyvissä yhteydenotoissa. (Tietosuojavaltuutetun toimisto 2025a.)

Viime vuosina sosiaalisen median palveluissa järjestettävät markkinointiarpajaiset ja kilpailut ovat yleistyneet Suomessa. Internetissä järjestettäviin arvontoihin ja kilpailuihin soveltuvat samat säännöt ja lait kuin ei-digitaalisessa maailmassa. Lisäksi sosiaalisen median kampanjoissa tulee noudattaa kyseisen palveluntarjoajan omia sääntöjä ja sopimusehtoja, jottei kampanja ole esimerkiksi mainostamista koskevien lakien tai yleistä tietosuoja-asetusta koskevien sääntöjen vastainen. (Koivumäki 2022, 139.)

Ongelmia voi ilmaantua esimerkiksi silloin kun järjestetään hashtag-arpajaiset tai -kilpailut, joissa pyydetään sosiaalisen median käyttäjiä julkaisemaan kuvia tietyllä hashtagilla. Tällöin vaarana on, että satunnainen sosiaalisen median käyttäjä voi tulla vahingossa osallistuneeksi kilpailuun, jonka kampanjaehdoissa lukee, että markkinoija saa rajoittamattomat oikeudet käyttää tietyllä hashtagilla julkaistuja kuvia ja aineistoja esimerkiksi somekanavissaan. Tämä on ongelmallista siksi, koska tiettyä hashtagia käyttävä sosiaalisen median julkaisija ei välttämättä ymmärrä antavansa esimerkiksi oman kuvansa markkinoijan hyödynnettäväksi. Siksi onkin suositeltavaa, että hashtag arvonnoissa ja kilpailuissa käytettäisiin sanayhdistelminä yrityksen nimeä ja sellaista sanaa, joka viestii

kaupallisesta kampanjasta. Lisäksi olisi hyvä, että kilpailun tai arvonnan aikana kampanjasta ja sen ehdoista tuotettaisiin paljon sisältöä yrityksen omiin sosiaalisen median kanaviin. (Koivumäki 2022, 141.)

3.6 Tietosuoja tapahtuman jälkeen

Planmeca Oy:n tietosuojavastaavan mukaan asiakastapahtuman jälkeen täytyy vielä huolehtia asianmukaisista toimista tietosuojaan liittyen. Esimerkiksi tarpeettomat henkilötiedot tulee poistaa viipymättä, palautteiden kerääminen asiakkailta tapahtumasta tulee suorittaa asianmukaisesti ja tapahtumaan osallistuneiden asiakkaiden henkilötiedot tulee liittää tarvittaessa joko asiakasrekisteriin tai potentiaalisten asiakkaiden rekisteriin. Asiakastapahtuman jälkeisissä toimissa tulee noudattaa kaikkia tietosuojasäännöksiä ja -periaatteita, joita opinnäytetyössä on esitelty ja käsitelty aiemmin.

3.6.1 Palautteen kerääminen

Planmeca Oy:n tietosuojavastaavan mukaan palautteen pyytäminen sähköisesti ei ole markkinointia vaan asiakasviestintää, eikä siksi edellytä ennakkosuostumusta. Tosin siitä on silti hyvä informoida tietosuojaselosteessa yhtenä tiedon käyttötarkoituksista. Jos tarkoituksena on kerätä potentiaalisia asiakkaita palautteen jättäneiden henkilötietojen avulla, kuluttajilta tulee palautteenannon yhteydessä kysyä lupa sähköiseen suoramarkkinointiin ja ilmoittaa mikäli tietoja aiotaan käyttää perinteiseen suoramarkkinointiin. Palautteita koskevat tilastot on kuitenkin hyvä käsitellä anonyymisti. Jos tapahtuman jälkeen palautteita pyydetään antamaan yrityksen omilla verkkosivuilla ilman asiakasviestintää, eikä mitään henkilötietoja kerätä, eikä palautteita voida yhdistää kehenkään tiettyyn henkilöön, niin silloin tietosuoja-asetusta ei sovelleta.

Joskus palautteen saamiseksi arvotaan palautteiden antaneiden kesken palkinto. Pelkästään arvontaa varten kerättyjä henkilötietoja ei saa käyttää muihin tarkoituksiin kuin arvonnan suorittamiseen ja palkinnon toimittamiseen.

3.6.2 Osallistujan liittäminen asiakasrekisteriin tai potentiaalinen asiakas -rekisteriin

Planmeca Oy:n tietosuojavastaavan mukaan silloin kun osallistuja ei ole vielä valmiiksi asiakasrekisterissä, B2B puolella ei edellytetä henkilön suostumusta hänen liittämiseensä asiakasrekisteriin tai potentiaalirekisteriin. Tämä johtuu siitä, että markkinointi yritysasiakkaille on sallittua myös sähköisesti ilman suostumusta. Mikäli jokin yritys on kieltänyt markkinoinnin, niin kieltoa on kuitenkin kunnioitettava. Silloin kun kyseessä on olemassa oleva yritysasiakas, asiakkuuteen liittyen on usein mielekästä tallentaa tieto siitä, mihin tilaisuuksiin ja asiakastapahtumiin hän on osallistunut. Tällöin asiakkaalle voidaan kohdentaa esimerkiksi asiakastapahtumaan osallistumiseen liittyviä

etuja ja alennuksia. Kuluttajapuolella henkilötietojen tallentamiseen ja suoramarkkinointiin on pyydettävä suostumus esimerkiksi tapahtuman ilmoittautumisvaiheessa.

3.6.3 Tarpeettomien henkilötietojen poisto

Laissa ei ole tämäntyyppisille tiedoille määriteltyä poistoaikaa, vaan säilytysaika määritellään käyttötarkoituksen mukaan. Eli käytännössä silloin kun henkilötiedot muuttuvat tarpeettomiksi, ne olisi hyvä poistaa viipymättä. Ruokavalinnat ja muut tapahtuman käytännönjärjestelyihin liittyvät osallistujien henkilökohtaiset tiedot ja valinnat olisi hyvä poistaa heti kun niitä ei enää tarvita. Jos tapahtumaan ilmoittautumisesta muodostuu lasku, tätä tietoa tulee kirjanpitolain mukaan säilyttää vähintään kuusi vuotta. (Lyyti 2024.)

Planmeca Oy:n tietosuojavastaavan mukaan tapahtumista nauhoitettavat webinaaritallenteet kannattaa anonymisoida, jos tallenteita säilytetään sisäisesti. Eli jos teams-webinaarissa osallistujien nimet ovat olleet näkyvillä, niin ne kannattaa jälkikäteen sumentaa tai rajata kuvasta pois. Tulostettujen ja sähköisten osallistujalistojen hävittämisestä tapahtuman jälkeen kannattaa sopia alihankkijoiden, kuten järjestysmiehiä tarjoavan palvelunjärjestäjän kanssa. Osallistujalistoilla voidaan tapahtuman aikana esimerkiksi varmistaa tapahtuman sisäänkäynnillä, ketkä ovat oikeutettuja osallistumaan tapahtumaan.

3.6.4 Tallenteen ja aineistojen jakaminen

Jos tapahtumasta jaetaan tallenteita tai muuta materiaalia osallistujille sähköpostitse, olisi hyvä, ettei sähköpostiviestin saajille tulisi ilmi kelle kaikille sähköpostiviesti on myös lähetetty. Materiaali olisi myös hyvä anonymisoida, jos se laitetaan jälkikäteen katseltavaksi esimerkiksi jollekin oppimisalustalle tai vastaavalle alustalle. Jos webinaaritallenteessa näkyvät siihen osallistuvien henkilöiden nimet, tästä olisi hyvä etukäteen informoida kaikkia webinaariin osallistuvia ennen webinaarin tallennusta ja jakamista (Halsvaha 27.5.2024, 29:00-29:40 min).

Planmeca Oy:n tietosuojavastaavan mukaan, jos tallenteen katselun yhteydessä tallentuu tieto siitä, kuka on katsellut tallennetta ja sen perusteella tehdään päätöksiä siitä, kehen otetaan yhteyttä myyntitarkoituksessa. Niin tästä on hyvä informoida tietosuojaperiaatteiden mukaisesti tallenteen jakamisen yhteydessä.

3.6.5 Kutsuminen seuraavaan tapahtumaan

Uuden tapahtumakutsun lähettämiseen sovelletaan samoja tietosuojaperiaatteita ja sääntöjä kuin opinnäytetyössä on aiemmin esitelty. Eli oikeus lähettää kutsu seuraavaan tapahtumaan riippuu siitä, onko tapahtumaan osallistunut henkilö asiakas, kuluttaja vai yritysasiakas ja siitä miten

seuraavan tapahtuman kutsu hänelle lähetetään. Jos tapahtumaan osallistunut henkilö on antanut suostumuksensa yhteystietojensa käyttöön tulevia tapahtuman markkinointitarkoituksia varten, voi hänelle edelleen lähettää markkinointimateriaalia tulevasta tapahtumasta (Lyyti 2024).

Planmeca Oy:n tietosuojavastaavan mukaan, henkilölle voi lähettää vuosittain kutsun vastaavanlaiseen tapahtumaan, jos henkilöä on informoitu vuosittaisesta kutsusta, eikä hän ole kieltänyt kutsun lähettämistä. Esimerkiksi asiakkaille ja jäsenille voi yleensä huolettaa lähettää kutsuja tapahtumiin, jos he eivät erikseen ole kertoneet, etteivät halua kutsuja. Kutsuja lähetellessä on hyvä muistaa, että kirjeissä ei saa näkyä muita henkilötietoja sen ulkopuolella kuin pelkästään tarvittavat tiedot kirjeen toimittamiseen, jotka ovat nimi ja osoite (Mehtonen 24.2.2024).

4 Hyvä opas

Organisaation toiminnan ytimessä on sen asiakkaille tuottamat tuotteet ja palvelut. Tämän vuoksi kaikkien työntekijöiden on hyvä tietää miten he voivat ottaa omassa työtehtävässään huomioon asiakkaiden tarpeet ja odotukset. Siksi työtehtävien onnistuneeseen suorittamiseen on hyvä tarjota opastusta. Työntekijöitä on tärkeä opastaa erilaisissa säännöissä, tekniikoissa ja toimintatavoissa, jotta he pystyvät keskittymään paremmin työnsä tekemiseen. Opastuksessa on tärkeä kiinnittää huomiota muun muassa tietoihin ja taitoihin mitä vaaditaan työtehtävien menestyksekkäisiin toteutuksiin. (Eklund 2023, 94–99.)

Hyvä opas vastaa kysymyksiin, joita sen lukijalla ei olisi tullut mieleenkään edes kysyä ennen oppaan lukemista. Oppaalla tulee olla myös selkeä kohderyhmä, kenen kysymyksiin se tarjoaa vastauksia. Oppaan tekstin tulee olla ymmärrettävää ja sen täytyy auttaa lukijaa ymmärtämään mistä oppaan teksteissä oikein on kyse. Pelkän tekstin lisäksi kokonaisuuteen voi sisältyä esimerkiksi asiantuntijoiden sitaatteja, case-esimerkkejä, vertailutaulukoita, vinkkilistoja, kuvitusta, oivaltavia ja helppoja lausahduksia sekä infograafeja. Lukijalle olisi hyvä myös kertoa mikä voisi olla mahdollinen seuraava askel oppaan lukemisen jälkeen. (Oiva 17.7.2017.)

4.1 Oppaan rakenne, värit, tausta, fonttivalinnat, kuvat ja symbolit

Sisällysluettelo on tärkeä osa opasta, koska se auttaa heti hahmottamaan mitä kaikkea opas sisältää (Oiva 17.7.2017). Aalto-Setälä ja Viitaila (2020) ovat sijoittaneet sisällysluettelonsa heti tietosuojaoppaansa kannen jälkeiselle sivulle. Aalto-Setälä ja Viitaila (2020) kertovat oppaansa alkupuolella sen tavoitteesta, yleisesti tietosuojasta sekä selvittävät lukijalle tärkeitä tietosuojaan liittyviä käsitteitä. Tietosuojaoppaassa kannattaa siis aluksi kertoa sen tavoite ja esitellä tietosuojaa yleisesti ja selventää siihen liittyviä keskeisiä käsitteitä. Oppaan tulisi edetä alun sisällysluettelon ja alustuksen jälkeen loogisesti. Oppaan loppupuolelle olisi hyvä varata mahdollisuuksien mukaan tilaa ”Usein kysytyt kysymykset -osiolle”, jossa annettaisiin vastauksia erilaisiin aiheeseen liittyviin kysymyksiin. (Tango Technology 23.3.2023.)

Värejä voidaan käyttää kuvailemaan tunnetiloja, luokittelemaan asioita ja kuvaamaan ympäröivää todellisuutta. Siksi esityksen värivalinnat eivät ole yhdentekeviä ja niillä voi olla ratkaiseva rooli siinä, kuinka mielekkäänä luettavana ja katseltavana materiaalia pidetään. Intensiteetiltään voimakkaita värejä ei tule käyttää suurilla pinnoilla niiden huomiovaikutuksen vuoksi. Tehostevärien on pysyttävä johdonmukaisesti samana koko materiaalin ajan. (Lammi 2015, 56–57.)

Kun edustetaan yritystä tai yhteisöä, sen tuottamien esitysmateriaalien ulkoasujen tulisi olla yhteneväisiä sen muiden tuotteiden graafisten ilmeiden kanssa. Esityksen väripalettia varten tarvitaan

3–5 eri perusväriä, joista voi käyttää lisäksi erilaisia vaaleampia tai tummempia kirkkausasteita. Perusvärien rinnalle on hyvä valita muutama tehosteväri, joita käytetään painoarvoa vaativissa kohdissa. Väripaletin kokoamiseen on olemassa erilaisia työkaluja netissä, joita kannattaa hyödyntää esityksen värivalintoja pohtiessa. (Lammi 2015, 59–61.)

Värivalintoja pohtiessa kannattaa muistaa, että väreillä saattaa olla oma erityismerkityksensä eri kulttuureissa. Esimerkiksi länsimaissa valkoinen edustaa puhtautta ja ylellisyyttä, mutta idässä väri yhdistetään kuolemaan. Länsimaisessa kulttuurissa keltainen koetaan myönteisenä ja eloisana, oranssi energisenä ja raikkaana, punainen aktiivisena ja päällekäyvänä, ruskea konservatiivisena ja tunnollisena, sininen rauhoittavana ja viileänä, vihreä pirteänä ja rauhoittavana, violetti arvokkaana ja mystisenä, musta ehdottomana ja synkkänä sekä harmaa itsenäisenä ja neutraalina. (Lammi 2015, 62.) Lisäksi tutkimusten mukaan ihmiset yhdistävät siniseen väriin luotettavuuden ja turvallisuuden, keltaiseen ja oranssiin väriin halpuuden ja hauskuuden, punaiseen nopeuden, mustaan laadun, violettiin rohkeuden, pelkoon punaisen ja mustan sekä korkealaatuisuuteen mustan, sinisen ja harmaan (Ruokolainen 2020, 123).

Esitysmateriaalin taustaan tulisi kiinnittää huomiota, koska se vaikuttaa siihen mitä muita värivalintoja sisällössä voi käyttää. Taustan ja sisällön välillä tulisi olla riittävästi kontrastia. Paras kontrasti syntyy tummalla tai vaalealla taustalla, josta muut värit erottuvat parhaiten. Jos materiaalista aiotaan tehdä esimerkiksi pieniä tulosteita, niin tumma tausta huonontaa usein luettavuutta. (Lammi 2015, 62–64.)

Esitysmateriaaleihin sopii parhaiten helposti luettavat fontit, jotka ovat yksinkertaisia ja pelkistettyjä. Päätteettömiä kirjasintyylejä, joiden kaikki viivat ovat suunnilleen yhtä paksuja kutsutaan groteskeiksi (sans serif). Groteskejä kirjasintyylejä ovat esimerkiksi *Arial, Helvetica* ja *Calibri*. Antiikvoiksi (serif) kutsutaan kirjasintyylejä, joissa kirjasintyyli on päätteellinen. Antiikvarisia kirjasintyylejä ovat esmerkiksi *Georgia* ja *Times New Roman*. Groteskisia kirjasintyylejä suositellaan tekstille, jota luetaan näytöltä. (Lammi 2015, 66–68.)

Työssä ei suositella käytettäväksi useampaa kuin kahta tai korkeintaan kolmea erilaista fonttia. Valituista fonteista yhtä käytetään otsikoissa ja alaotsikoissa ja toista pidemmissä tekstikokonaisuuksissa. Fonttivalinnasta tulee harmoninen, muodollinen ja rauhallinen kun työssä käytetään yhtä fonttia ja sen eri pistekokoja ja leikkauksia. Konflikti syntyy silloin kun työssä käytetään liian samankaltaisia fontteja, joissa ei ole tarpeeksi suurta kontrastia. Mikäli halutaan käyttää kahta erilaista fonttia, kannattaa kirjasintyyleiksi valita antiikva sekä groteski. (Lammi 2015, 68–69.)

Kuvia kannattaa käyttää koska, kuvat helpottavat parhaimmillaan tekstin ymmärtämistä, kuvat jäävät tekstiä paremmin mieleen ja ovat tekstiä tehokkaampia vaikuttamaan ihmisen tunteisiin. Kuvaa

valitessa pitää kuitenkin kiinnittää huomiota siihen, että se liittyy asiayhteyteen ja vahvistaa tekstin viestiä. Esimerkiksi kuva ihmisistä herättää yleensä positiivisia reaktioita. Lisäksi leikkisä ja muuten aiheeseen liittyvä yllättävä kuva voi olla joskus toimiva lähestymistapa käsiteltävään aiheeseen. Mikäli hyvää kuvaa ei löydy, kannattaa se jättää suosiolla pois. (Lammi 2015, 88–90.) Valokuvien sijasta materiaalissa voi käyttää myös symboleja, jotka välittävät viestejä parhaimmillaan yksiselitteisemmin kuin valokuvat. Symbolit parantavat materiaalin silmäiltävyyttä, sillä symbolit ilmaisevat asioita tiiviisti ilman sanoja. (Lammi 2015, 94.)

4.2 Saavutettavuus

Saavutettavuudella tarkoitetaan sitä, että informaatio esitetään sellaisessa muodossa, jossa se on kaikkien saatavilla. Tekstisisällön tulisi olla esimerkiksi mahdollisimman selkeästi luettavissa, jotta ihmiset, joilla on rajoitteita näkemisen kanssa, pystyisivät lukemaan tekstiä mahdollisimman hyvin. Oikeanlaisilla värivalinnoilla, fonteilla ja tekstin asetteluilla erilaisista sisällöistä pystytään tekemään saavutettavampia. Usein toimijoita velvoittaa saavutettavuusdirektiivi, mutta kaikkien yritysten olisi hyvä tähdätä saavutettavuuteen toiminnassaan. Saavutettavuudella pystymme lisäämään kaikkien ihmisten osallisuutta yhteiskunnan eri toimintoihin sekä oikeudenmukaisuutta ja yhdenvertaisuutta. Tämän vuoksi saavutettavuus on myös arvovalinta, joka kannattaisi huomioida, kun tuotetaan esimerkiksi digitaalisia palveluja, fyysisiä dokumentteja tai tulosteita. (Kansallinen Sivistysliitto ry 2023, 4–5.)

Saavutettavassa tekstisisällössä tärkeää on ensiksi kertoa pääasia ja sen jälkeen vasta taustatiedot ja perustelut. Itse teksti kannattaa esittää sopivan pieninä kokonaisuuksina tarpeeksi isoin rivivälein ja kappalevälein, koska tyhjä tila helpottaa tekstin lukemista. Kirjasinkokoon kannattaa kiinnittää huomiota ja valita tarpeeksi suuri fontti. Tekstin ja taustan värien välillä olisi hyvä olla tarpeeksi suuri kontrasti. Suuraakkosten sijaan kannattaa suosia pienaakkosia, koska niitä on helpompi lukea. Lisäksi kannattaa välttää kursivointeja, alleviivauksia ja suuraakkosia. Kuvassa 1 havainnollistetaan mitä asioita kannattaa välttää ja suosia saavutettavamman materiaalin tuottamiseksi. (Kansallinen Sivistysliitto ry 2023, 6–8.)

Kuva 1. Suosi ja vältä näitä kirjasintyyppejä saavutettavuuden parantamiseksi (mukaillen Kansallinen Sivistysliitto ry 2023, 9)

5 Tietosuojaopas Planmeca Oy:lle

Toiminnallisen opinnäytetyön tavoitteena oli luoda tietosuojaopas asiakastapahtumien järjestämisiä varten Planmeca Oy:lle. Aloitin opinnäytetyön suunnittelun 2024 lokakuussa, ja pidimme ensimmäinen palaverin tietosuojaoppaan sisällöstä marraskuun puolessa välissä Planmeca Oy:n tietosuoja-asiantuntijoiden kanssa. Tietoperustan keräämisen sekä kirjoittamisen aloitin marraskuun lopulla ja sain sen päätökseen helmikuun alussa.

Toisen palaverin Planmeca Oy:n tietosuoja-asiantuntijoiden kanssa pidimme helmikuun alussa. Palaverissa kävimme läpi kerättyä tietoperustaa ja ideoimme tietosuojaoppaan olemusta. Sovimme, että teen oppaan hyödyntäen Canvaa, joka on ilmainen graafiseen suunnitteluun tarkoitettu verkkotyökalu. Kävimme toisen palaverin jälkeen vielä keskusteluja tietosuojaoppaan sisällöistä liittyen muun muassa usein kysyttyihin kysymyksiin. Tietosuojaopas valmistui maaliskuussa ja se on tarkoitus julkaista Planmeca Oy:n sisäisessä verkossa kesän aikana. Kuvassa 2 havainnollistetaan toiminnallisen opinnäytetyön aikataulullista etenemistä.

Tietosuojaoppaan toteutus 2024 - 2025		
Vaihe 1	Viikko 42 - 45	Opinnäytetyön ja tietosuojaoppaan tekemisen suunnittelua
Vaihe 2	Viikko 46	Ensimmäinen palaveri Planmecan kanssa, jossa tietosuojaoppaan ideointia yhdessä
Vaihe 3	Viikko 47 - 6	Tietoperustan kerääminen
Vaihe 4	Viikko 6	Toinen palaveri Planmecan kanssa jossa tietosuojaoppaan ideointia yhdessä
Vaihe 5	Viikko 6 - 9	Tietosuojaoppaan tekeminen Canvalla
Vaihe 6	Viikko 10	Palautetta tietosuojaoppaasta
Vaihe 7	Viikko 11	**Valmis tietosuojaopas**

Kuva 2. Tietosuojaoppaan toteutuksen vaiheet

5.1 Lähtötilanteen kuvaus

Tietosuojaopas asiakastapahtumia varten tehtiin Planmeca Oy:n tietosuojatoimistolle, jonka tehtäviin kuuluu muun muassa yrityksen työntekijöiden ohjeistaminen tietosuojaan liittyvissä tilanteissa. Planmeca Oy on yksi maailman johtavista terveysteknologian laitevalmistajista, jonka tuotteita viedään yli 120 maahan. Planmeca Oy on Planmeca Groupin emoyhtiö, joka työllistää maailmanlaajuisesti lähes 4400 henkilöä. Konsernin liikevaihto oli 1,2 miljardia euroa vuonna 2023. Planmeca Oy:n tuotevalikoimaan kuuluu muun muassa erilaisia hampaiden hoitokoneita, 2D- ja 3D-kuvantamislaitteita sekä niihin kuuluvia ohjelmistoratkaisuja. (Planmeca Oy s.a.)

Yleisen tietosuojasetuksen osoitusvelvollisuuden mukaan rekisterinpitäjän, eli Planmeca Oy:n, on pystyttävä osoittamaan, että se noudattaa tietosuojaperiaatteita kaikissa henkilötietojen käsittelyn vaiheissa. Tämän vuoksi yrityksen tietosuojakäytänteistä tulisi olla olemassa dokumentit, joissa neuvotaan ja ohjeistetaan työntekijöitä erilaisissa henkilötietojen käsittelyä vaativissa tilanteissa. Planmeca Oy järjestää ajoittain asiakastilaisuuksia ja muita tapahtumia, joiden vuoksi tietosuojaoppaan tekeminen oli tärkeää, jotta osoitusvelvollisuus täyttyisi.

Lisäksi Planmeca Oy toimii terveysteknologia alalla, jossa asiakkaiden luottamus konserniin on ensiarvoisen tärkeää. Tietosuojan pettämisestä saattaisi aiheutua mainehaittoja, jotka voisivat pahimmillaan vaikuttaa hyvinkin paljon Planmeca Oy:n liikevaihtoon. Siksi tietosuojaoppaan aluksi lukijalle kerrotaan, että opas ja sen sisältö on tehty asiakkaiden luottamuksen säilyttämistä varten. Kuvassa 3 esitellään tietosuojaoppaan sivua, jossa kerrotaan, mitä varten opas on tehty.

Tietosuojatoimisto Tietosuoja ohjekirja

Mitä varten ohjekirja on tehty?

Asiakkaiden luottamusta varten!

Tietosuojan toteutuminen on tärkeää aina kun ollaan asiakkaiden kanssa tekemisissä. Tietosuojan pettäessä, asiakkaiden luottamus yritystä kohtaan voi murentua pahimmillaan jopa sekunneissa. Tämän vuoksi tapahtumien järjestelyissä on hyvä kiinnittää erityistä huomiota asiakkaiden henkilötietojen turvalliseen käsittelyyn.

Kun asiakkaalle tulee tunne, että hänestä välitetään, voi tämä tunne muuntautua kilpailueduksi, jolla yritys saadaan menestymään kilpailijoitaan paremmin.

Tämä opas ei luonnollisestikaan tule vastaamaan kaikkiin tapahtumien tietosuojaan liittyviin kysymyksiin, mutta se antaa hyvät lähtökohdat tietosuojallisen tapahtuman järjestämiseen.

Opas antaa tietoa:

- **Tietosuojasta** — Oppaan avulla tutustut tietosuojan perusteisiin, jotka on aina hyvä huomioida kun käsitellään henkilötietoja.
- **Tapahtumien tietosuojasta** — Oppaassa on kuvattu erilaisia tapahtumien järjestämiseen liittyviä tietosuojatilanteita.
- **Usein kysyttyihin kysymyksiin** — Oppaan lopussa on usein kysytyille kysymyksille varattuna oma osionsa.
- **Esimerkein** — Opas sisältää esimerkkejä erilaisista tilanteista, joissa tietosuoja tulee huomioida.

02

Kuva 3. Tietosuojaoppaan toinen sivu, jossa esitellään miksi tietosuojaopas on tehty

5.2 Suunnittelun keskeiset menetelmät ja onnistumisen mittaaminen

Toiminnallisen opinnäytetyöntyön kehittämistyön menetelmänä toimi konstruktiivinen tutkimus. Konstruktiivinen tutkimus toimii hyvin silloin kun tavoitteena on luoda yritykselle jokin konkreettinen tuotos, kuten opas. Tuotos pyrkii muuttamaan kohdeyrityksen käytänteitä ja toimintatapoja aikaisempia paremmiksi. Tässä kehittämistyön menetelmässä korostuu ammattikirjallisuuden ja muiden lähteiden hyödyntäminen sekä yhteistyö tutkimuksen tuotoksen hyödyntäjien, eli yrityksen työntekijöiden kanssa. Tyypillisiä menetelmiä tuotoksen aikaan saamiseksi ovat ryhmäkeskustelut ja haastattelut. (Ojasalo, Moilanen & Ritalahti 2015, 65–68.)

Valitsin tietosuojaoppaan kehittämistyön menetelmäksi konstruktiivisen tutkimuksen, koska se tuntui eri vaihtoehtoja pohdittuani luontevimmilta. Tietosuojaopasta varten ei tarvitse tuottaa mitään

uutta tietoa, vaan kerätä ja yhdistää eri lähteistä tarpeelliset tiedot yhdeksi toimivaksi kokonaisuudeksi. Oppaan sisällöstä käytiin myös ryhmäkeskusteluja Planmeca Oy:n tietosuoja-asiantuntijoiden kanssa, joiden tarpeisiin opas tehtiin.

Toisena menetelmänä tietosuojaoppaan toteuttamiseen käytin benchmarkingia. Benchmarkingin perusideana on tutkia menestyvien yritysten toimintatapoja, ja ottaa toimintatavoista hyväksi havaittuja tapoja omaan käyttöön (Ojasalo ym. 2015, 186). Yritin tutkia muita tietosuojaoppaita suunnitellakseni omaani, mutta en onnistunut löytämään opasta, joka olisi keskittynyt pelkästään asiakastapahtumien tietosuojaan. Pidin kuitenkin Aalto-Setälän ja Viitailan (2020) TIETOSUOJA PÄHKINÄNKUORESSA - Tietosuojaopas yrityksille tavasta avata tietosuojaan liittyvät keskeiset käsitteet lukijalle oppaan alussa. Kuvassa 4 havainnollistetaan toiminnallisen opinnäytetyön tuotoksena syntyneen oppaan yhtä tietosuojasanastoon keskittyvän osuuden sivuista.

Tietosuojatoimisto Tietosuoja ohjekirja

1.1 Mikä ihmeen GDPR?

GDPR (General Data Protection Regulation) on EU:n vuonna 2018 säätämä yleinen tietosuoja-asetus, jonka tarkoituksena on parantaa ihmisten yksityisyyden suojaa sekä ohjeistaa yrityksiä henkilötietojen turvallisessa käsittelyssä.

Osa tietosuojaan liittyvistä termeistä saattaa olla hankala ymmärtää. Joten tässä oppaan osiossa keskitytään pelkästään tietosuojaan liittyvien käsitteiden määrittelemiseen.

1.2 Tietosuojasanasto

Alikäsittelijä on taho, joka käsittelee henkilötietoja henkilötietojen käsittelijän puolesta. Jotta alikäsittelijä voidaan hyödyntää, pitää rekisterinpitäjän tai yhteisrekisterinpitäjän antaa tähän kirjallinen hyväksyntä.

Anonymisoinnilla tarkoitetaan henkilötietojen käsittelyä pysyvästi siten, että tietoja ei pystytä enää yhdistämään kehenkään tiettyyn henkilöön. Anonymisoinnin jälkeen tietoja ei enää katsota henkilötiedoiksi, joten niiden käsittelyä eivät enää rajoita tietosuojasäännökset.

Erityisiin henkilötietoryhmiin kuuluvat arkaluontoiset henkilötiedot, joiden käsittely yrityksissä ja muissa organisaatioissa on alustavasti kiellettyä ilman tiettyjä perusteita. Erityisiin henkilötietoryhmiin kuuluvat muun muassa tiedot ihmisen rodusta tai etnisestä alkuperästä, sukupuolisesta suuntautumisesta, poliittisista mielipiteistä, uskonnollisista tai filosofisista vakaumuksista, ammattiliittoon kuulumisesta sekä geneettiset, biometriset tai terveydelliset tiedot.

Evästeillä digitaalisen palvelujen tarjoaja seuraa selaimen käyttäjän toimintaa esimerkiksi linkkien käytöstä ja muista valinnoista. Evästeitä ja niihin liittyvää seurantateknologiaa ei saa käyttää sivustolle tultaessa, vaan siihen tulee kysyä sivuston käyttäjältä lupa. Tietoja saa kerätä vain silloin kun siihen on suostuttu ja tiedot ovat välttämättömiä digitaalisen palvelun, kuten esimerkiksi verkkokaupan ostoskorin toimimiseksi.

Henkilötietoja ovat kaikki ne tiedot, joiden perusteella henkilö voidaan tunnistaa joko suoraan tai välillisesti yhdistämällä henkilöä kuvaavan tieto johonkin toiseen tietoon. Henkilötietoja ovat esimerkiksi nimi, asuinosoite, henkilötunnus, puhelinnumero, sähköpostiosoite, ihmisen valokuva, ihmisen ääni, IP-osoite, auton rekisterinumero, passin numero, kulttuurinen profiili ja opiskelijatiedot. Henkilötietoja eivät ole esimerkiksi yrityksen rekisteritunnus ja organisaation yleinen sähköpostiosoite.

Henkilötietojen käsittelijä on ulkopuolinen henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Ulkopuolinen henkilö voi olla esimerkiksi alihankkija tai yhteistyökumppani, jolle rekisterinpitäjä on ulkoistanut tietojen käsittelyä, kuten säilyttämistä. Henkilötietojen käsittelijä toimii rekisterinpitäjän antamien ohjeiden mukaan, eikä hän saa itsenäisesti päättää tietojen keräämisestä tai käytöstä.

06

Kuva 4. Kuvakaappaus tietosuojaoppaan yhdestä tietosuojasanastoon keskittyvästä sivusta

Toiminnallisen opinnäytetyön tuotoksena syntyneen tietosuojaoppaan onnistumisen mittarina voidaan pitää Planmeca Oy:n tietosuojavastaavan tyytyväisyyttä oppaaseen. Palavereissa sovimme, että tietosuojaoppaan sisältö pysyttelisi yleisellä tasolla, eikä siihen laitettaisi Planmeca Oy:ssä työskentelevien ihmisten nimiä, ammattinimikkeitä, sovelluksia tai muita yrityksen käytäntöjä. Toive johtui siitä, että tietosuojaopas on löydettävissä avoimesta julkaisuarkistosta Theseuksesta, jossa säilytetään Suomen ammattikorkeakoulujen opinnäytetöitä. Lisäksi tietosuojavastaavan toiveena oli tehdä tietosuojaoppaasta pdf-muotoinen, koska se on ympäristöystävällinen ja sen pystyisi tallentamaan Planmeca Oy:n sisäiseen verkkoon. Tietosuojaoppaan valmistumisaikataulun suhteen Planmeca Oy:n tietosuojavastaavalla ei ollut toiveita, koska hän halusi antaa minulle työrauhan oppaan kanssa.

5.3 Tietosuojaoppaan sisällön tuottaminen

Planmeca Oy:n tietosuojatoimistossa ei ole aikaisemmin tehty tietylle tarkasti rajatulle kohderyhmälle ja tilanteelle omia visuaalisia tietosuojaoppaita. Sen vuoksi opinnäytetyönä valmistuneen tietosuojaoppaan tekemiseen ei ole voinut katsoa mallia aikaisemmista oppaista. Tietosuojaoppaan kohderyhmänä olivat muun muassa Planmeca Oy:n markkinointi- ja viestintäosasto sekä muut toimihenkilöt ketkä osallistuvat asiakastapahtumien henkilötietojen käsittelyyn.

Toiminnallisen opinnäytetyön tuotoksen eli tietosuojaoppaan työvaiheisiin kuului yksinkertaisuudessaan tietoperustan tekeminen ja oppaan luominen näiden pohjalta. Tietoperusta syntyi hyvin pitkälti alan kirjallisuutta ja erilaisia verkkosivuja tutkimalla. Tuotoksen luomiseen tarvittiin verkkosivustojen ja kirjojen tutkimisen lisäksi palautetta ja ryhmäkeskusteluja Planmeca Oy:n tietosuoja-asiantuntijoiden kanssa. Tällä tavoin tietosuojaohjeistus saatiin vastaavaan mahdollisimman hyvin Planmeca Oy:n tietosuojatoimiston tarpeita.

Tietosuojaoppaasta tuli laaja kokonaisuus, koska perehdyin huolella aiheeseen ymmärtääkseni mitä tietosuoja on, ja keräsin paljon materiaalia tietosuojasta opasta varten opinnäytetyön tietoperustaan. Tietoperustasta poimin tärkeimmiksi kokemani asiat tietosuojaoppaaseen. Rajasin opinnäytetyöstä pois Euroopan unionin ulkopuolella tapahtuvan henkilötietojen käsittelyn, koska muuten tietosuojaoppaasta olisi tullut aivan liian iso kokonaisuus asiakastapahtumien järjestäjille esimerkiksi yhdellä kertaa luettavaksi ja sisäistettäväksi.

Ideoin oppaan sisällöksi myös esimerkkitapahtuman kuvitteellisesta asiakastapahtumasta, minkä terveysteknologiayhtiö voisi mahdollisesti järjestää. Esimerkkitapahtumaan liittyen tiivistin oppaan sisällön siltä osin, mitä kyseisessä tapahtumassa olisi hyvä huomioida tietosuojan käsittelyyn liittyen. Kuvassa 5 näkyy tietosuojaoppaan esimerkkitapahtumaan liittyvät sivut.

04
Muistilistoja & esimerkkejä

4.1 Tietosuojallisen asiakastilaisuuden muistilista

Kuvitellaan, että terveysteknologia alalla toimiva suomalainen yritys X Oy on järjestämässä **asiakastilaisuuden** pääkonttorillaan, jonne se on kutsumassa alan yrityksiä testaamaan X Oy:n uusia myyntiin tulevia röntgenlaitteita. Tapahtuma kestää kaksi päivää ja tilaisuudessa vierailleille tarjoillaan hienoja ruokia ja juomia, sekä tapahtumasta tehdään X Oy:n someen julkaisuja. Tilaisuudesta kerätään myös palautetta.

- Osallistujia tulee informoida mihin tarkoitukseen heidän henkilötietoja käytetään ja kuinka kauan tietoja tullaan säilyttämään.
- Tapahtumalle kannattaa mahdollisesti tehdä oma tietosuojaseloste.
- Tapahtuman henkilötietojen käsittelyä suunniteltaessa kannattaa olla tarvittaessa yhteydessä yrityksen tietosuoja-asiantuntijoihin, kuten tietosuojavastaavaan.

Ennen tapahtumaa

- Yrityksille saa lähettää markkinointimateriaalia tapahtumasta sähköpostitse, soittamalla tai tekstiviestitse
- Henkilöille, jotka ovat ostaneet samankaltaisia tuotteita X Oy:ltä, saa lähettää tapahtumasta markkinointimateriaalia sähköpostitse ja tekstiviestein, jos he eivät ole sitä erikseen kieltäneet.
- Tietojenkäsittelysopimukset täytyy tehdä ulkopuolisten yritysten (kuten valokuvaajan ja catering-palvelun) kanssa, jotka tulevat käsittelemään osallistujien henkilötietoja.
- Markkinointiviestien mukaan tulee laittaa tietosuojainformaatio ja kertoa kielto-oikeudesta
- Osallistujia on Informoitava ja mahdollisesti kysyttävä suostumusta, mikäli heidän henkilötietoja tulee näkymään esimerkiksi webinaareissa tai nimilapuissa muille osallistujille.
- Jos tapahtumaa mainostetaan X Oy:n nettisivuilla sijaintitietoja hyödyntäen, täytyy tietojen hyödyntämiseen kysyä lupa nettisivulle tultaessa.
- Tietojen minimoinnin periaate, eli kerää osallistujilta vain oikeasti tarpeellista tietoa
- Kysy suostumusta arkaluontoisten tietojen (esim. tiedot allergioista) säilyttämiseen.

Tapahtuman aikana

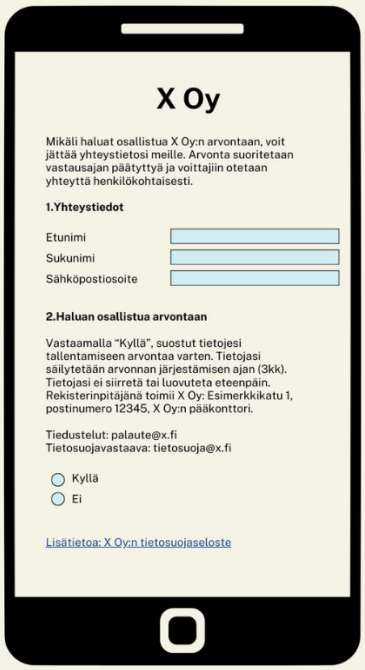
- Vieraita, jotka ovat antaneet luvan kuvaamiselle ilmoittautumisen yhteydessä, saa kuvata.
- Vapaaehtoinen asettautuminen kuvattavaksi tapahtumaan rakennetun kuvausseinän eteen, käy suostumukseksi siihen, että kuva voidaan julkaista somessa.
- Mikäli tapahtumasta otetusta yleiskuvasta ei pysty tunnistamaan erityisesti ketään henkilöä, saa kuvan esimerkiksi jakaa sosiaalisessa mediassa, ilman etukäteen kysyttyä lupaa.
- Arvontojen ja kilpailujen yhteydessä saa kerätä vain oikeasti tarpeellisia tietoja kilpailun tai arvonnan suorittamiseksi. Jos kerättyjä henkilötietoja aiotaan käyttää sähköiseen suoramarkkinointiin, tähän täytyy kysyä erikseen lupa rekisteröidyltä.
- Hashtag arvonnoissa ja kilpailuissa olisi hyvä käyttää sanayhdistelmiä, jotka viestivät kaupallisesta kampanjasta.

Tapahtuman jälkeen

- Palautteen pyytäminen sähköisesti on sallittua, mutta siitä on silti hyvä informoida tietosuojaselosteessa yhtenä tiedon käyttötarkoituksista.
- Jos osallistuja ei ole vielä valmiiksi asiakasrekisterissä, B2B puolella ei edellytetä henkilön suostumusta hänen liittämiseensä asiakasrekisteriin tai potentiaalirekisteriin.
- Tapahtuman jälkeen kaikki tarpeettomiksi muuttuneet henkilötiedot on poistettava viipymättä.
- Webinaaritallenteesta tulee jälkikäteen anonymisoida, eli sumentaa tai rajata osallistujien nimet pois kuvasta, vaikka tallenne säilytettäisiin pelkästään sisäistä käyttöä varten.
- Jos vieras ei ole kieltäytynyt, voi hänelle lähettää markkinointimateriaalia tulevasta ensi vuoden tapahtumasta.

4.2 Esimerkki arvontalomakkeesta

Kuvitellaan, että X Oy lähettää asiakastilaisuuden jälkeen siihen osallistuneille henkilöille palautekyselyn. Jos palautekyselyn yhteydessä on mahdollisuus osallistua arvontaan, niin arvontalomake voi näyttää esimerkiksi tältä.



X Oy

Mikäli haluat osallistua X Oy:n arvontaan, voit jättää yhteystietosi meille. Arvonta suoritetaan vastausajan päätyttyä ja voittajiin otetaan yhteyttä henkilökohtaisesti.

1.Yhteystiedot

Etunimi
Sukunimi
Sähköpostiosoite

2.Haluan osallistua arvontaan

Vastaamalla "Kyllä", suostut tietojesi tallentamiseen arvontaa varten. Tietojasi säilytetään arvonnan järjestämisen ajan (3kk). Tietojasi ei siirretä tai luovuteta eteenpäin. Rekisterinpitäjänä toimii X Oy: Esimerkkikatu 1, postinumero 12345, X Oy:n pääkonttori.

Tiedustelut: palaute@x.fi
Tietosuojavastaava: tietosuoja@x.fi

○ Kyllä
○ Ei

Lisätietoa: X Oy:n tietosuojaseloste

Kuva 5. Tietosuojaoppaan sisältö on tiivistetty "Muistilistoja & esimerkkejä" lukuun

Oppaan sisällössä on myös huomioitu se, että Planmeca Oy:n markkinointimateriaaleissa ja laitteistojen opetusmateriaaleissa käytetään oikeiden potilaiden röntgenkuvia. Röntgenkuvat luetaan arkaluontoisiksi henkilötiedoiksi, joten niiden käsittelyssä tulee olla erityisen huolellinen. Kuvassa 6 on oppaan sivu, jossa keskitytään arkaluontoisten henkilötietojen käsittelyyn.

Tietosuojatoimisto Tietosuoja ohjekirja

Erityisten henkilötieto-ryhmien käsittely

Erityisiä henkilötietoryhmiä eli arkaluontoisia tietoja, kuten ammattiliiton jäsenyyttä tai terveyttä koskevia tietoja, ei pääsääntöisesti saa käsitellä ollenkaan, ellei käsittelyyn ole olemassa jokin hyväksyttävä peruste, kuten tietosuoja-asetuksessa sallittu poikkeus tai muu laillinen peruste. Rekisteröidyn nimenomaisella suostumuksella rekisterinpitäjä voi käsitellä arkaluontoisia henkilötietoja yhtä tai useampaa käyttötarkoitusta varten, ellei lainsäädäntö estä tätä yksiselitteisesti.

Mikäli asiakkaiden arkaluontoisten henkilötietojen käsittely on tarpeellista organisaatiossa, niin tietojen käsittelyyn ja säilyttämiseen tulee pyytää asiakkaiden **suostumus**. Ongelmia voi syntyä silloin kun joistakin tiedoista voi välillisesti käydä ilmi asiakkaan arkaluontoisia tietoja. Esimerkiksi erityisruokavaliosta voi päätellä henkilön terveydentilaan liittyviä tietoja.

Jos tällaisia tietoja tallennetaan pysyvästi asiakasrekisteriin, kannattaa tähän ehdottomasti pyytää rekisteröidyltä suostumus. Mikäli yrityksessä käsitellään arkaluontoisia tietoja, joiden käsittelyyn ei ole asiakkailta lupaa, ne pitää poistaa välittömästi tai pyytää rekisteröidyiltä lupa jälkikäteen.

Terveysteknologia yhtiöt käyttävät markkinointimateriaalissaan usein potilaskuvia, jotka luokitellaan arkaluontoisiksi henkilötiedoiksi.

14

Kuva 6. Kuvakaappaus tietosuojaoppaan arkaluontoisten henkilötietojen käsittelyä koskevasta sivusta

5.4 Tietosuojaoppaan rakenteen muotoilu

Tietosuojaoppaan rakenne muotoiltiin mahdollisimman yksinkertaiseksi ja helposti lähestyttäväksi sen lukijalle. Aluksi tietosuojaoppaassa kerrotaan lukijalle, miksi opas on oikein tehty. Tämän jälkeen sisällysluettelo näyttää mitä tietosuojaopas pitää sisällään. Kuvassa 7 on näkyvillä tietosuojaoppaan sisällysluettelo. Sisällysluetteloa seuraa tietosuojasanasto, josta lukija voi tarvittaessa

tarkistaa hänelle epäselvät tietosuojaan liittyvät sanat. Tietosuojasanaston jälkeen oppaassa käsitellään tietosuojan perusteita sekä tietosuojaohjeita tapahtumiin. Teoriaan keskittyvän osuuden jälkeen tietosuojaoppaassa kootaan yhteen oppaan tärkein sisältö ”Muistilistoja ja esimerkkejä” -lukuun. Tietosuojaopas loppuu ”Usein kysytyt kysymykset” -lukuun, josta lukija voi mahdollisesti saada vastauksia häntä askarruttaviin kysymyksiin.

Tietosuojatoimisto Tietosuoja ohjekirja

Sisällys luettelo

03

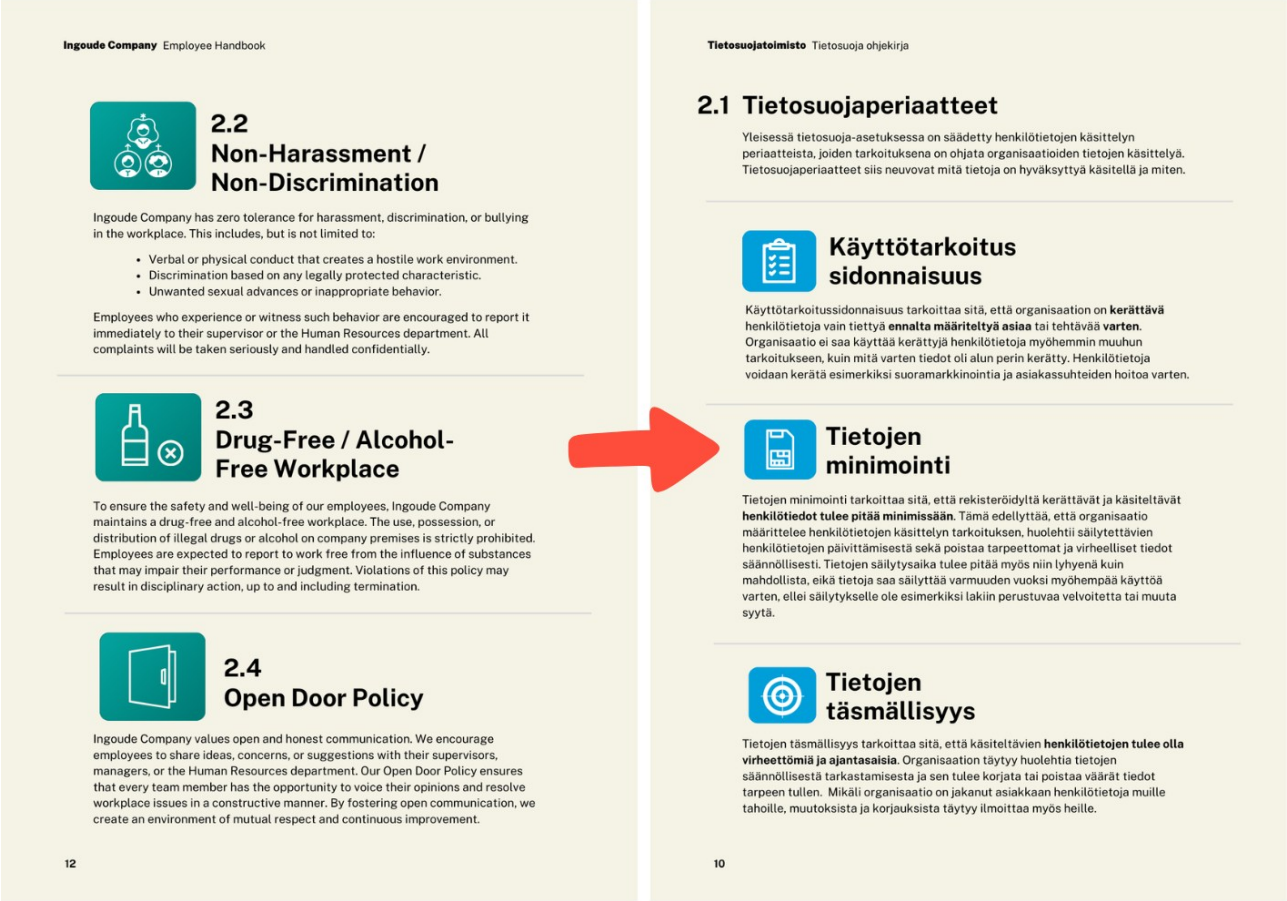
Tietosuojatoimisto Tietosuoja ohjekirja

04

Kuva 7. Tietosuojaoppaan sisällysluettelo

5.5 Tietosuojaoppaan visuaalisen ilmeen toteutus

Tietosuojaoppaan visuaalisen ilmeen työstäminen aloitettiin etsimällä graafisen suunnittelun verkkotyökalu Canvasta mallipohja, johon pystyttäisiin lisäämään tietosuojaoppaaseen valitut tekstit ja sisällöt. Sopivan mallipohjan löydyttyä, sen asettelut, kuvat ja värit korvattiin osittain paremmin tietosuojaan liittyvillä kuvavaihtoehdoilla ja väreillä. Tietosuojaoppaan fonttina säilytettiin Canvan mallipohjan Public Sans fontti johtuen sen yksinkertaisesta ja pelkistetystä muodosta, joka teki fontista helposti luettavan. Kuvassa 8 näkyy kuinka Canvan mallipohjan tekstit, tyyli ja värit on korvattu omilla teksteillä, tyylillä ja väreillä.



Kuva 8. Kuvan vasemmalla puolella on näkyvissä Canvan mallipohjan sivu, josta on muokattu tietosuojaoppaan oikean puoleinen sivu

Virtanen (2020, 61) neuvoo käyttämään julkaisuissa 2-3 väriä, joista yksi väri saa olla yrityksen logon väri. Valitsin tietosuojaoppaaseen perusväreiksi Planmeca Oy:n tietosuojatoimiston logon väreistä vaaleansinisen ja muiksi perusväreiksi keltaisen, oranssin ja tummansinisen. Mielestäni luotettavuutta ilmaisevan sinisen värin kanssa oppaaseen sopivat keltainen ja oranssi, koska niitä pidetään länsimaisessa kulttuurissa myönteisinä ja raikkaina väreinä. Kuvassa 9 esitellään tietosuojaoppaan kansi, jossa valitut perusvärit näkyvät.

Kuva 9. Vasemmalla kuvassa ovat tietosuojaoppaaseen valitut perusvärit ja oikealla tietosuojaoppaan kansi

Oppaan tehosteväriksi valikoitui vaaleansininen, koska se kuuluu Planmeca Oy:n tietosuojatoimiston logoon. Tehosteväri korostaa tekstissä tärkeitä kohtia sekä huomioita ja nostaa ne paremmin taustasta esiin. Tietosuojaoppaan taustaväriksi valikoitui todella vaalea ja pehmeä keltaisen sävy, joka löytyi valmiiksi valitsemastani Canvan mallipohjasta.

Tietosuojaoppaassa on käytetty paljon erilaisia havainnollistavia kuvia, symboleita ja taulukoita. Valituissa kuvissa on pyritty huomioimaan Planmeca Oy, eli tietosuojaoppaan kuvitukseen pyrittiin löytämään terveysteknologiaan, toimistotyöhön ja tapahtuman järjestämiseen liittyviä kuvia. Kuvaan 10 on kerätty tietosuojaoppaan sivuja, joissa on erilaisia havainnollistavia kuvia ja taulukoita.

2.4 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjä on aina viime kädessä vastuussa tietosuojalainsäädännön toteutumisesta sen omassa toiminnassa, sekä henkilötietojen käsittelijöiden toiminnassa.

Mikäli rekisterinpitäjä hyödyntää asiakastapahtumassa ulkopuolisia **henkilötietojen käsittelijöitä**, kuten valokuvaajaa tai catering-palvelua, täytyy heidän käsitellä henkilötietoja rekisterinpitäjän antamien ohjeiden mukaisesti. Heidän kanssaan tulee myös laatia sopimus, josta selviää osapuolten velvollisuudet liittyen henkilötietojen käsittelyyn. Jos henkilötietojen käsittelijä haluaa käyttää apunaan muita käsittelijöitä, tähän täytyy saada kirjallinen lupa rekisterinpitäjältä.

Rekisterinpitäjän kuuluu myös huolehtia organisaation teknisistä ja organisatorisista toimenpiteistä, kuten tietoturvasta, joilla varmistetaan henkilötietojen turvallinen käsittely.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet

Sisäänrakennetulla ja oletusarvoisella tietosuojalla (privacy by design ja privacy by default) tarkoitetaan näkökulmaa, jossa tietosuojan periaatteiden toteutuminen huomioidaan organisaation palvelun, sovelluksen tai tapahtuman koko elinkaaren ajaksi aina alun suunnitteluvaiheesta tietojen poistamiseen saakka.

Tietosuojan huomioiminen ei ole pelkästään esimerkiksi tietosuojavastaavan vastuulla, vaan kaikkien henkilöiden, joiden työhön liittyy henkilötietojen käsittelyä tai käsittelyn suunnittelua.

Yhteisrekisterinpitäjyys

Yhteisrekisterinpitäjyydessä, kahden tai useamman organisaation tulee yhdessä määritellä omat vastuualueensa henkilötietojen käsittelystä sekä rekisteröityjen oikeuksien toteuttamisesta ja tiedottamisesta. Yhteisrekisterinpitäjien roolit tulee olla rekisteröityjen saatavilla esimerkiksi tietosuojaselosteen muodossa.

Tietoturvaloukkauksen seuraukset

Tietoturvaloukkausta epäiltäessä tietosuojavaltuutettu voi pyrkiä muokkaamaan organisaation henkilötietojen käsittelyä tietosuojalainsäädännön mukaiseksi erilaisin keinoin.

Tietosuojavaltuutettu voi korjaavana toimina esimerkiksi varoittaa rekisterinpitäjää kyseenalaisista aiotuista käsittelytoimista, antaa huomautuksen vääränlaisista käsittelytoimista, määrätä organisaatio ilmoittamaan tietoturvaloukkauksesta rekisteröidyille, asettaa väliaikaisen tai pysyvän henkilötietojen käsittelykiellon, määrätä hallinnollisen seuraamusmaksun tai määrätä tiedonsiirron keskeyttämisestä kolmannessa maassa sijaitsevaan organisaatioon.

Jos jokin epäilyttää henkilötietojen käsittelyssä, niin älä epäröi olla yhteydessä organisaation tietosuojavastaavaan.

3.4 Suoramarkkinointi ja asiakasviestintä

Perinteisellä suoramarkkinoinnilla tarkoitetaan puhelimitse tai postitse tapahtuvaa markkinointia. **Sähköisellä suoramarkkinoinnilla** tarkoitetaan markkinointia, joka tapahtuu sähköisesti esimerkiksi automatisoitujen soittojärjestelmien, faxien, sähköpostiviestien, tekstiviestien, puheviestien, ääniviestien tai kuvaviestien välityksellä.

Asiakasviestintänä pidetään viestintää, jonka tarkoituksena on asiakassuhteen hoitamiseksi tarvittava yhteydenpito, mihin ei liity markkinointia. Organisaatio saa itse valita mitä tapaa, kuten esimerkiksi sähköpostia ja tekstiviestiä, se käyttää asiakasviestinnässään. Asiakkaalla ei ole laillista oikeutta kieltäytyä häntä koskevasta asiakasviestinnästä.

Organisaatio saa lähettää asiakkailleen ja jäsenilleen asiakasviestintää **uutiskirjeinä**, kunhan ne eivät sisällä mainoksia. Suoramarkkinointia sisältävän uutiskirjeen lähettämiseen vaaditaan vastaanottajalta lupa.

Markkinointiviesteihin täytyy muistaa laittaa mukaan **tietosuojainformaatio** esimerkiksi linkin muodossa sekä kertoa viestin vastaanottajalle **kielto-oikeudesta**. Sähköposteihin voi laittaa esimerkiksi "klikkaa tästä, jos et halua jatkossa vastaanottaa viestejämme" -linkin. Tekstiviesteissä kielto-oikeudesta voi kertoa esimerkiksi "Kiellot: 0800 xxxx" tekstillä viestin lopussa. Puhelusta ei saa periä erillistä maksua.

Kuluttajalle saa tehdä markkinointia perinteisillä menetelmillä vapaasti ilman ennakkosuostumusta. Kuluttaja voi kuitenkin halutessaan kieltää markkinoinnin ja hänelle tulee kertoa kielto-oikeudesta asiakassuhteen tai muun yhteydenpidon aloitushetkellä esimerkiksi tietosuojaselosteen avulla.

Myyntipuhelun tai tapahtumakutsun hyväksyminen puhelimessa edellyttää kuluttajalta kirjallista jälkivahvistusta soiton jälkeen. Kirjallinen jälkivahvistus voi olla esimerkiksi tekstiviesti, johon vastaamalla kuluttaja hyväksyy tarjouksen tai osallistumisen tapahtumaan. Mikäli asiakas on itse yhteydessä yritykseen tai on jättänyt yhteydenottopyynnön yritykselle, ei jälkivahvistusta tarvita.

Markkinointipuheluja saa nauhoittaa puhelun sisällön todentamiseksi sekä koulutustarkoitusta tai laadun tarkkailua varten. Asiakkaalle tulee kertoa nauhoittamisesta mahdollisimman pian puhelun alettua.

Kuluttajalle ja potentiaaliselle asiakkaalle saa tehdä sähköisiä viestimiä hyödyntäen tarjouksia, vain silloin kun hän on antanut siihen **etukäteen suostumuksensa**.

Lupapyyntöjä varten kuluttajalle pitää antaa tarpeeksi informaatiota käsittelyn tarkoituksista ja tavoista sekä minkälaista suoramarkkinointia (viikkokirje, tarjous, kutsut jne.) hän tulisi saamaan, jotta hän voi arvioida mihin on suostumassa. Esimerkiksi EU:n tietosuojaviranomaisten mukaan sähköpostin ja tekstiviestin lähettämisestä tulisi kysyä lupa kahdella erillisellä kysymyksellä.

Lupapyyntöjä ei tarvita **poikkeuksellisesti** silloin kun palvelun tarjoaja tai tuotteen myyjä lähettää asiakkaalle sähköistä suoramarkkinointia omista samaan tuoteryhmään kuuluvista palveluista tai tuotteista esimerkiksi sähköpostitse tai tekstiviestinä. Palvelun tarjoajan tai tuotteen myyjän on kuitenkin täytynyt saada asiakkaan yhteystiedot palvelun tai tuotteen myynnin yhteydessä.

Yritysten yhteyshenkilöihin saa olla yhteydessä ilman etukäteen annettua suostumusta niin perinteisen kuin sähköisen suoramarkkinoinnin keinoin, kunhan yhteydenotot liittyvät jollain tavalla yrityksen toimintaan. Suoramarkkinointi tulee kuitenkin lopettaa, mikäli vastaanottaja kieltää sen.

Yrityksille ei saa lähettää kuluttajille suunnattua markkinointia, vaan suoramarkkinointiviestin sisällön pitää olla kohderyhmälle sopiva.

Mahdollisesta sähköisestä asiakasviestinnästä asiakkaalle, kuten lähetyksen tilanteen ilmoittamisesta tekstiviestillä, olisi suositeltavaa informoida kuluttajaa jo henkilötietoja kerättäessä, vaikka lainsäädännön puitteissa sitä ei vaadita. Selkeä informointi viestintäkäytännöistä kasvattaa asiakkaiden luottamusta organisaatiota kohtaan.

Tapahtuman markkinointi ja asiakasviestintä

Asiakastapahtuman markkinointia koskevat samat säännöt kuin suoramarkkinointia ja asiakasviestintää. **Kuluttajille** tapahtumakutsun lähettäminen kirjeitse tai siitä puhelimitse tiedottaminen on sallittua ilman ennakkosuostumusta. Sähköpostimarkkinointi edellyttää ennakkosuostumuksen.

Yrityksille tapahtumakutsun lähettäminen kirjeitse tai sähköpostitse on sallittua ilman ennakkosuostumusta. Myös puhelinmarkkinointi tapahtumasta on sallittua. Yrityksille kannattaa lähettää puhelimessa sovitusta tapahtumaan osallistumisesta esimerkiksi linkki sähköpostiin, jossa yritys voi käydä vahvistamassa osallistumisensa.

Sallittu suoramarkkinointi ja asiakasviestintä	B2C	B2B
Perinteinen suoramarkkinointi ilman ennakkosuostumusta	✓	✓
Sähköinen suoramarkkinointi ilman ennakkosuostumusta	✗	✓
Sähköinen suoramarkkinointi ennakkosuostumuksella	✓	✓
Mahdollinen asiakasviestintä sähköisesti ja perinteisesti	✓	✓

Kuva 10. Tietosuojaoppaan sivuilla on erilaisia havainnollistavia kuvia ja taulukoita

6 Pohdinta

Opinnäytetyön tavoitteena oli luoda Planmeca Oy:lle tietosuojaopas asiakastapahtumien järjestämisiä varten. Opinnäytetyössä hyödynnettiin konstruktiivista kehittämistyön menetelmää, joka oli mielestäni sopivin menetelmä tietosuojaoppaan aikaansaamiseksi. Menetelmään kuului tietosuojaan liittyvän ammattikirjallisuuden, viranomaissivuston ja muiden lähteiden hyödyntämisen lisäksi palaverit Planmeca Oy:n tietosuoja-asiantuntijoiden kanssa.

Opinnäytetyön tuotosta, eli tietosuojaopasta tehdessä ymmärsin, että tietosuojan perusteiden hallitsemisella pääsee jo todella pitkälle henkilötietojen onnistuneessa käsittelyssä asiakastapahtumia järjestettäessä. Tietojen minimoinnin ja käyttötarkoitussidonnaisuuden periaatteita noudattamalla asiakastapahtuman järjestäjä pienentäisi tietosuojaan liittyviä riskejä jo huomattavasti. Riskit madaltuisivat entisestään, jos asiakastapahtuman järjestäjä tunnistaisi mitkä kaikki tiedot luokitellaan henkilötiedoksi, ja osaisi tarvittaessa pyytää neuvoa yrityksen tietosuojavastaavalta henkilötietojen käsittelemisen ja keräämisen eri vaiheissa.

Ymmärsin myös, että henkilötiedon käsittelyn perusteista rekisteröidyn suostumus on asiakastapahtuman järjestäjän, eli rekisterinpitäjän näkökulmasta yksi käyttökelpoisimmista käsittelyperusteista. Asiakastapahtuman järjestäjä pääsee helpoimmalla tietosuojan näkökulmasta, kun se kysyy osallistujalta eli rekisteröidyltä esimerkiksi ilmoittautumisen yhteydessä suostumusta tietojen säilyttämiseen, kohdennettuun mainontaan verkkosivustolla, suoramarkkinointiin, tapahtumassa kuvaamiseen tai oikeastaan mihin tahansa toimeen mitä asiakastapahtuman osallistujan tiedoilla aiotaan tehdä. Tämä johtuu siitä, että suostumuksen tulee olla vapaaehtoinen ja tietoisesti tehty, joten se ei jätä rekisterinpitäjälle tai rekisteröidylle epäselvyyttä esimerkiksi mihin tarkoituksiin rekisterinpitäjä saa käyttää rekisteröidyn luovuttamia tietoja asiakastapahtumaan liittyen.

Oivalsin myös, että henkilötietojen käsittelyn läpinäkyvyys on tärkeää, jotta asiakastapahtumaan osallistuvat henkilöt pystyisivät luottamaan siihen, että heidän tietojaan käsitellään asianmukaisesti. Läpinäkyvyys lisää asiakastapahtumaan osallistuvan henkilön luottamusta yritystä kohtaan, joka on tärkeää terveysteknologia alalla. Läpinäkyvyyttä pystytään edistämään esimerkiksi ajantasaisilla tietosuojaselosteilla ja antamalla rekisteröidylle informaatiota hänen henkilötietojensa käsittelystä sekä oikeuksista. Rekisterinpitäjä voi lisätä asiakkaiden luottamusta noudattamalla tietosuojaperiaatteita, huolehtimalla omista velvollisuuksistaan ja käsittelemällä asiakkaiden henkilötietoja luottamuksellisesti ja tietoturvallisesti.

6.1 Työn hyödynnettävyys ja ajankohtaisuus

Yleinen tietosuoja-asetus on ollut voimassa jo useamman vuoden ja tuntuu, että monilla yrityksillä ja organisaatioilla on edelleen vaikeuksia toimia vastuullisesti tietosuojan puitteissa. Esimerkiksi moni kotimainen yritys ja kaupunki on ollut esillä uutisissa negatiiviseen sävyyn tietosuojan laiminlyömisistä viime aikoina. Siksi opinnäytetyönä syntynyt tietosuojaopas on erittäin ajankohtainen, koska olisi hyvä, että jokainen suomalainen yritys saisi tietosuojakäytäntönsä kuntoon vastaamaan yleisen tietosuoja-asetuksen vaatimuksia, ennen kuin ePrivacy-asetus astuu voimaan. EPrivacy-asetus tulee korvaamaan vanhan ePrivacy-direktiivin, sitten kun asetuksen sisällöistä on päästy sopuun.

Mielestäni opinnäytetyön tuotoksena syntynyt tietosuojaopas on todella hyödynnettävä. Planmeca Oy järjestää erilaisia asiakas- ja tutustumistilaisuuksia pääkonttorilla Helsingissä, joten oppaasta on varmasti apua näiden tapahtumien tietosuojallisessa järjestämisessä. Lisäksi muutkin yritykset voivat hyödyntää tietosuojaopasta apuna omien tapahtumien järjestelyissä, johtuen sen yleisluontoisesta tyylistä.

6.2 Opinnäytetyön luotettavuus ja jatkokehittämisehdotukset

Koen opinnäytetyönä syntyneen tietosuojaoppaan luotettavaksi, koska sen lähteinä on käytetty ammattikirjallisuutta ja tietosuojavaltuutetun toimiston verkkosivuja. Lisäksi Planmeca Oy:n tietosuoja-asiantuntijat ovat tarkastaneet tietosuojaoppaan ja antaneet palautetta oppaan sisällöstä. Toki täytyy muistaa, että yleinen tietosuoja-asetus ei aina anna suoria vastauksia kaikkiin henkilötietojen käsittelyä koskeviin kysymyksiin ja tulevaisuudessa lait ja niiden tulkinnat voivat muuttua. Joten tulevaisuudessa tietosuojaopasta saattaa joutua päivittämään hyvinkin pian sen julkaisun jälkeen.

Jatkokehittämisehdotuksena asiakastapahtumiin keskittyvälle tietosuojaoppaalle ideoisin muihin tilanteisiin keskittyviä tietosuojaoppaita. Vastaavia oppaita voisi tehdä esimerkiksi myyntitilanteiden henkilötietojen käsittelystä tai yrityksen työntekijöiden henkilötietojen käsittelystä. Tulevien oppaiden pohjana voisi käyttää opinnäytetyönä syntynyttä tietosuojaopasta ja korvata asiakastapahtumien järjestämiseen liittyvät osuudet muilla henkilötietojen käsittelyyn keskittyvillä osuuksilla.

6.3 Oman oppimisen ja onnistumisen arviointi

Opinnäytetyön tekemisen aikana opin paljon tietosuojasta. Huomasin muun muassa ymmärtäväni miksi eri nettisivuilla vieraillessani puhelimeni näytölle lävähtää aina ”Yksityisyytesi on meille tärkeää” -teksti, jonka lopussa pystyy valikoimaan, hylkääkö vai hyväksyykö verkkosivun evästeiden käytön. On ollut hienoa huomata myös se, että nykyään törmätessäni yritysten tietosuojaan liittyviin

uutisiin, ymmärrän mitä oikein on tapahtunut, mitä tietosuojaperiaatetta tai rekisteröidyn oikeuksia on rikottu ja mitä esimerkiksi käsitteet rekisterinpitäjä ja tietosuojavaltuutettu tarkoittavat.

Opinnäytetyöprosessin aikana olisin voinut kuitenkin tehdä joitain asioita paremmin. Olisin voinut pyytää esimerkiksi enemmän ohjeita ja palautetta tietosuojaoppaasta Planmeca Oy:n tietosuoja-asiantuntijoilta, jolloin oppaasta olisi varmasti tullut nykyistä parempi. Lisäksi minun olisi ehkä kannattanut tehdä opas jollain muulla ohjelmalla kuin Canvalla, koska kyseisellä ohjelmalla on omat rajoitteensa, jotka mielestäni hieman näkyivät tietosuojaoppaan ulkoasussa esimerkiksi tekstin tasauksessa. Olisin jälkeenpäin ajateltuna voinut käyttää enemmän englanninkielisiä lähteitä tietoperustan luomisessa, jolloin olisin ehkä löytänyt sellaista tietoa mitä ei löydy suomenkielisistä lähteistä. Tietosuojaoppaasta olisi voinut myös mahdollisesti yrittää tehdä hieman lyhyemmän kuin siitä tuli, mutta toisaalta oppaassa on ehkä mieluummin liian paljon tietoa, kuin liian vähän.

Kaiken kaikkiaan opinnäytetyön tekeminen sujui hyvin ja onnistuin mielestäni tuottamaan onnistuneen tietosuojaoppaan asiakastapahtumia varten Planmeca Oy:lle. Pysyin opinnäytetyön valmistumisen suhteen myös suurin piirtein aikataulussa. Luulen, että osaan tämän opinnäytetyöprosessin jälkeen jatkossa kiinnittää aivan eri tavalla huomiota tietosuojaan ja henkilötietojen käsittelyyn, kuin jos olisin valinnut jonkin tyypillisemmän markkinoinnin ja viestinnän aihepiirin opinnäytetyöni aiheeksi. Olen kuitenkin tyytyväinen opinnäytetyöni aiheen valintaan, koska tietosuojasta huolehtiminen kuuluu kaikille ja se tulee olemaan myös minun vastuullani, missä tahansa työssä tai organisaatiossa tulevaisuudessa työskentelenkin.

Lähteet

Aalto-Setälä, M. & Viitaila, M. 2020. TIETOSUOJA PÄHKINÄNKUORESSA - Tietosuojaopas yrityk-sille. Keskuskauppakamari. Helsinki. Luettavissa: https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf. Luettu: 22.10.2024.

Andreasson, A. Oravala, J. & Toivonen, M. 2023. Tietosuoja ja yksityisyys: Opas jokaiselle. Tietosanoma. Helsinki.

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). 2., päivitetty laitos. Tietosanoma. Helsinki.

Data Protection Commission Ireland. 28.2.2020. Does the GDPR Really Say That? – Attendee Lists and Name Tags. Blogi. Luettavissa: https://www.dataprotection.ie/en/dpc-guidance/blogs/does-gdpr-really-say-attendee-lists-and-name-tags. Luettu: 30.1.2025.

Dixit, V. 18.11.2024. Legal Considerations for Webinars: Privacy, Copyright, and Beyond. Virtuaalisten tapahtumien järjestämiseen keskittyneen yrityksen Airmeet Inc Blogi. Luettavissa: https://www.airmeet.com/hub/blog/legal-considerations-for-webinars-privacy-copyright-and-beyond/. Luettu: 29.1.2025.

Eklund, A. 2023. Tervetuloa meille! Uuden työntekijän perehdytys. 3. painos. Brik Impact. Espoo. E-kirja. Luettu: 31.1.2025.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

European Data Protection Board. Rekisterinpitäjä vai henkilötietojen käsittelijä. Luettavissa: https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_fi. Luettu: 23.11.2024.

Halsvaha, T. 27.5.2024. Tunnetko tapahtumien tietosuojan. Lyyti -Tapahtumanhallintajärjestelmän YouTube -kanava. Webinaari. Katsottavissa: https://www.youtube.com/watch?v=7Iqckvz6RME. Katsottu: 28.1.2025.

Hanninen, M. Laine, E. Rantala, K. Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Kauppakamari. Helsinki. E-kirja. Luettu: 24.10.2024.

Järvinen, P. 2022. Digiajan tietosuoja: turvaa henkilötietosi, torju identiteettivarkaudet, suojaudu urkinnalta. Tammi. Helsinki.

Kansainvälinen kauppakamari ICC. 2018. KANSAINVÄLISEN KAUPPAKAMARIN ICC:N MARKKINOINTISÄÄNNÖT 2018. Luettavissa: https://kauppakamari.fi/wp content/uploads/2020/05/marketing-code-finnish-saannot-suomeksi-2019.pdf. Luettu: 7.1.2024.

Kansallinen Sivistysliitto ry. 3.1.2023. Opas saavutettavan viestinnän tekemiseen. Kansio. Helsinki. Luettavissa: https://www.kansio.fi/wp-content/uploads/2023/01/saavutettavuusopas-netti.pdf. Luettu: 31.1.2025.

Keller, M. 2023. Mitä on tietosuoja? Alma Talent. Helsinki.

Koivumäki, E. 2022. Markkinointijuridiikka. Uudistettu painos. Kauppakamari. Helsinki. E-kirja. Luettu: 7.1.2025.

Korpisaari, P. Pitkänen, O. & Warma-Lehtinen, O. 2022. Tietosuoja. 2., uudistettu painos. Alma Talent. Helsinki. E-kirja. Luettu: 20.11.2024.

Krakau, T. & Haapalehto, S. 2020. Tietopyynnöt ja henkilötietojen luovuttaminen: Opas julkisuuslain mukaisten tietopyyntöjen ja tietosuoja-asetuksen mukaisten henkilötietojen tarkastuspyyntöjen käsittelyyn sekä muihin tietojen luovutuksiin. Alma Talent. Helsinki. E-kirja. Luettu: 1.12.2024.

Kuusimaa, K. 1.3.2017. Näkökohtia profiloinnista uudessa tietosuoja-asetuksessa. IAB:n blogi. Luettavissa: https://www.iab.fi/uutiset-blogi/iablogi/iablogi/nakokohtia-profiloinnista-uudessa-tietosuoja-asetuksessa.html. Luettu: 19.1.2025.

Lammi, O. 2015. Viesti & Vaikuta: Käsikirja presentaatioiden pitäjälle. Docendo. Jyväskylä.

Lindfelt, V. 9.11.2022. Tietosuojaselosteen laatiminen – tarkistuslista asiakirjan laatijalle. Lakitoimisto Lakiuksen blogi. Luettavissa: https://www.lakius.fi/kirjoituksia/tietosuojaselosteen-laatiminen-tarkistuslista. Luettu: 10.1.2025.

Lindfelt, V. 2025. Tietojenkäsittelysopimus (DPA). Luettavissa: https://www.lakius.fi/tietojenkasittelysopimus-dpa. Luettu: 12.1.2025.

Lyyti 2024. Tapahtumajärjestäjän 39 GDPR-kysymystä ja vastausta. Luettavissa: https://help.lyyti.com/hc/fi/articles/360000810834-Tapahtumaj%C3%A4rjest%C3%A4j%C3%A4n-39-GDPR-kysymyst%C3%A4-ja-vastausta. Luettu: 28.1.2025.

Mehtonen, J. 24.2.2024. Sairaalasta lähetettiin asiakkaalle kirje, jonka ikkunasta näkyi terveystietoja – ”Kyseessä voi olla tietoturvaloukkaus”. Yle. Luettavissa: https://yle.fi/a/74-20075998. Luettu: 30.1.2025.

Oiva, M. 17.7.2017. Eri sisältölajit, osa 2 koukuttava opas. Differon sisällöntuotantoon keskittyvä blogi. Luettavissa: https://www.differo.fi/blogi/eri-sisaltolajit-osa-2-koukuttava-opas. Luettu: 31.1.2025.

Ojasalo, K. Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Sanoma Pro Oy. Helsinki. E-kirja. Luettu: 30.10.2024.

Planmeca Oy. s.a. Yritys. Planmeca Better care through innovation. Luettavissa: https://www.planmeca.com/fi/yritys/. Luettu: 28.2.2025.

Ruokolainen, P. 2020. Brändikäsikirja: Näin teet yritysbrändistä vetovoimaisen! Kauppakamari. Helsinki. E-kirja. Luettu: 1.2.2025.

Siney, B. 8.6.2018. What am I allowed to do with business cards under GDPR? Be Secure Consultants blogi. Luettavissa: https://besecure-consultants.com/i-allowed-business-cards-gdpr/. Luettu: 30.1.2025.

Tango Technology. 23.3.2023. 9 Steps To Create Effective How-To Guides in 2023. Tango Technology blogi. Luettavissa: https://www.tango.ai/blog/how-to-guides#create-outline. Luettu: 31.1.2025.

Tietosuojalaki 5.12.2018/1050

Tietosuojavaltuutetun toimisto. 2024a. Usein kysyttyä EU:n tietosuoja-asetuksesta. Luettavissa: https://tietosuoja.fi/usein-kysyttya-gdpr. Luettu: 22.10.2024

Tietosuojavaltuutetun toimisto. 2024b. Verkkokauppa.comille seuraamusmaksu asiakastietojen säilytysajan määrittelemättä jättämisestä – myös vaatimus asiakkaan rekisteröitymisestä oli lainvastainen. Tiedote. Luettavissa: https://tietosuoja.fi/-/verkkokauppa.comille-seuraamusmaksu-asiakastietojen-sailytysajan-maarittelematta-jattamisesta-myos-vaatimus-asiakkaan-rekisteroitymisesta-oli-lainvastainen. Luettu: 22.10.2024.

Tietosuojavaltuutetun toimisto 2024c. Osoita noudattavasi tietosuojasäännöksiä. Luettavissa: https://tietosuoja.fi/osoitusvelvollisuus. Luettu: 24.11.2024.

Tietosuojavaltuutetun toimisto. 2024d. Tietosuoja. Luettavissa: https://tietosuoja.fi/tietosuoja. Luettu: 21.11.2024.

Tietosuojavaltuutetun toimisto. 2024e. Rekisteröidyn suostumus. Luettavissa: https://tietosuoja.fi/rekisteroidyn-suostumus. Luettu: 21.11.2024.

Tietosuojavaltuutetun toimisto 2024f. Tietojen täsmällisyys. Luettavissa: https://tietosuoja.fi/tietojen-tasmallisyys. Luettu: 28.11.2024.

Tietosuojavaltuutetun toimisto 2024g. Säilytyksen rajoittaminen. Luettavissa: https://tietosuoja.fi/sailytyksen-rajoittaminen. Luettu: 28.11.2024.

Tietosuojavaltuutetun toimisto 2024h. Luottamuksellisuus ja turvallisuus. Luettavissa: https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus. Luettu: 29.11.2024.

Tietosuojavaltuutetun toimisto 2024i. Milloin henkilötietoja saa kerätä? Luettavissa: https://tietosuoja.fi/kasittelyperusteet. Luettu: 1.12.2024.

Tietosuojavaltuutetun toimisto 2024j. Rekisterinpitäjän oikeutettu etu. Luettavissa: https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu. Luettu: 3.12.2024.

Tietosuojavaltuutetun toimisto 2024k. Henkilötietojen käsittelijän velvollisuudet. Luettavissa: https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet. Luettu: 4.12.2024.

Tietosuojavaltuutetun toimisto 2024l. Oikeus saada tietoja henkilötietojen käsittelystä. Luettavissa: https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta. Luettu: 12.12.2024

Tietosuojavaltuutetun toimisto 2024m. Oikeus saada tutustua tietoihin. Luettavissa: https://tietosuoja.fi/oikeus-saada-tutustua-tietoihin. Luettu:12.12.2024.

Tietosuojavaltuutetun toimisto 2024n. Oikeus oikaista tietoja. Luettavissa: https://tietosuoja.fi/oikeus-oikaista-tietoja. Luettu: 13.12.2024.

Tietosuojavaltuutetun toimisto 2024o. Oikeus poistaa tiedot. Luettavissa: https://tietosuoja.fi/oikeus-poistaa-tiedot. Luettu: 13.12.2024.

Tietosuojavaltuutetun toimisto 2024p. Oikeus rajoittaa tietojen käsittelyä. Luettavissa: https://tietosuoja.fi/oikeus-rajoittaa-kasittelya. Luettu: 14.12.2024.

Tietosuojavaltuutetun toimisto 2024q. Oikeus siirtää tiedot järjestelmästä toiseen. Luettavissa: https://tietosuoja.fi/oikeus-siirtaa-tiedot. Luettu: 16.12.2024.

Tietosuojavaltuutetun toimisto 2024r. Oikeus vastustaa tietojen käsittelyä. Luettavissa: https://tietosuoja.fi/oikeus-vastustaa-kasittelya. Luettu: 16.12.2024.

Tietosuojavaltuutetun toimisto 2024s. Automaattinen päätöksenteko ja profilointi. Luettavissa: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi. Luettu: 16.12.2024.

Tietosuojavaltuutetun toimisto 2025a. Usein kysyttyä suoramarkkinoinnista. Luettavissa: https://tietosuoja.fi/usein-kysyttya-suoramarkkinointi. Luettu: 20.1.2025.

Virtanen, S. 2020. Somemarkkinoinnin työkirja. Kauppakamari. Helsinki. E-kirja. Luettu: 5.2.2025.

Voutilainen, T. 2023. Digitaalisten palvelujen sääntely. 2., uudistettu painos. Alma Talent. Helsinki. E-kirja. Luettu: 22.11.2024.

Väyrynen, P. 3.2.2022. Some-markkinoinnin tietosuoja yrityksissä | Pirjo Väyrynen, Pirannava Intelligence. TIEKE Tietoyhteiskunnan kehittämiskeskus ry:n YouTube-kanava. video. Katsottavissa: https://www.youtube.com/watch?v=JA-zgk0R_wc. Katsottu: 22.1.2025.

Liitteet

Liite 1. Tietosuoja ohjekirja – Opas tietosuojallisten asiakastapahtumien järjestämiseen

Tietosuojatoimisto

Tietosuoja ohjekirja

Opas tietosuojallisten asiakastapahtumien järjestämiseen

Julkaistu **Kesä 2025**

Versio **2025 Painos**

Mitä varten ohjekirja on tehty?

Asiakkaiden luottamusta varten!

Tietosuojan toteutuminen on tärkeää aina kun ollaan asiakkaiden kanssa tekemisissä. Tietosuojan pettäessä, asiakkaiden luottamus yritystä kohtaan voi murentua pahimmillaan jopa sekunneissa. Tämän vuoksi tapahtumien järjestelyissä on hyvä kiinnittää erityistä huomiota asiakkaiden henkilötietojen turvalliseen käsittelyyn.

Kun asiakkaalle tulee tunne, että hänestä välitetään, voi tämä tunne muuntautua kilpailueduksi, jolla yritys saadaan menestymään kilpailijoitaan paremmin.

Tämä opas ei luonnollisestikaan tule vastaamaan kaikkiin tapahtumien tietosuojaan liittyviin kysymyksiin, mutta se antaa hyvät lähtökohdat tietosuojallisen tapahtuman järjestämiseen.

Opas antaa tietoa:

Tietosuojasta	Oppaan avulla tutustut tietosuojan perusteisiin, jotka on aina hyvä huomioida kun käsitellään henkilötietoja.
Tapahtumien tietosuojasta	Oppaassa on kuvattu erilaisia tapahtumien järjestämiseen liittyviä tietosuojatilanteita.
Usein kysyttyihin kysymyksiin	Oppaan lopussa on usein kysytyille kysymyksille varattuna oma osionsa.
Esimerkein	Opas sisältää esimerkkejä erilaisista tilanteista, joissa tietosuoja tulee huomioida.

Sisällys luettelo

01 Tietosuoja-sanastoa

1.1 Mikä ihmeen GDPR?

GDPR (General Data Protection Regulation) on EU:n vuonna 2018 säätämä yleinen tietosuoja-asetus, jonka tarkoituksena on parantaa ihmisten yksityisyyden suojaa sekä ohjeistaa yrityksiä henkilötietojen turvallisessa käsittelyssä.

Osa tietosuojaan liittyvistä termeistä saattaa olla hankala ymmärtää. Joten tässä oppaan osiossa keskitytään pelkästään tietosuojaan liittyvien käsitteiden määrittelemiseen.

1.2 Tietosuojasanasto

Alikäsittelijä on taho, joka käsittelee henkilötietoja henkilötietojen käsittelijän puolesta. Jotta alikäsittelijä voidaan hyödyntää, pitää rekisterinpitäjän tai yhteisrekisterinpitäjän antaa tähän kirjallinen hyväksyntä.

Anonymisoinnilla tarkoitetaan henkilötietojen käsittelyä pysyvästi siten, että tietoja ei pystytä enää yhdistämään kehenkään tiettyyn henkilöön. Anonymisoinnin jälkeen tietoja ei enää katsota henkilötiedoiksi, joten niiden käsittelyä eivät enää rajoita tietosuojasäännökset.

Erityisiin henkilötietoryhmiin kuuluvat arkaluontoiset henkilötiedot, joiden käsittely yrityksissä ja muissa organisaatioissa on alustavasti kiellettyä ilman tiettyjä perusteita. Erityisiin henkilötietoryhmiin kuuluvat muun muassa tiedot ihmisen rodusta tai etnisestä alkuperästä, sukupuolisesta suuntautumisesta, poliittisista mielipiteistä, uskonnollisista tai filosofisista vakaumuksista, ammattiliittoon kuulumisesta sekä geneettiset, biometriset tai terveydelliset tiedot.

Evästeillä digitaalisen palvelujen tarjoaja seuraa selaimen käyttäjän toimintaa esimerkiksi linkkien käytöstä ja muista valinnoista. Evästeitä ja niihin liittyvää seurantateknologiaa ei saa käyttää sivustolle tultaessa, vaan siihen tulee kysyä sivuston käyttäjältä lupa. Tietoja saa kerätä vain silloin kun siihen on suostuttu ja tiedot ovat välttämättömiä digitaalisen palvelun, kuten esimerkiksi verkkokaupan ostoskorin toimimiseksi.

Henkilötietoja ovat kaikki ne tiedot, joiden perusteella henkilö voidaan tunnistaa joko suoraan tai välillisesti yhdistämällä henkilöä kuvaavan tieto johonkin toiseen tietoon. Henkilötietoja ovat esimerkiksi nimi, asuinosoite, henkilötunnus, puhelinnumero, sähköpostiosoite, ihmisen valokuva, ihmisen ääni, IP-osoite, auton rekisterinumero, passin numero, kulttuurinen profiili ja opiskelijatiedot. Henkilötietoja eivät ole esimerkiksi yrityksen rekisteritunnus ja organisaation yleinen sähköpostiosoite.

Henkilötietojen käsittelijä on ulkopuolinen henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Ulkopuolinen henkilö voi olla esimerkiksi alihankkija tai yhteistyökumppani, jolle rekisterinpitäjä on ulkoistanut tietojen käsittelyä, kuten säilyttämistä. Henkilötietojen käsittelijä toimii rekisterinpitäjän antamien ohjeiden mukaan, eikä hän saa itsenäisesti päättää tietojen keräämisestä tai käytöstä.

Henkilötietojen käsittelyllä tarkoitetaan lähes kaikenlaisia toimintoja, joissa on mukana henkilötietoja. Käsittely voi olla esimerkiksi tietojen keräämistä, säilyttämistä, muokkaamista, luovuttamista, yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Kolmannella osapuolella tarkoitetaan jotain muuta henkilöä kuin rekisterinpitäjää, henkilötietojen käsittelijää, rekisteröityä tai muuta henkilöä, joka käsittelee henkilötietoja rekisterinpitäjän vastuun alaisena ja jolla on oikeus siihen.

Profiloinnilla tarkoitetaan toimintaa, jossa rekisterinpitäjä tallentaa ja analysoi automaattisen päätöksenteon avulla rekisteröidystä tietoja, joiden perusteella esimerkiksi arvioidaan tai ennustetaan hänen kykyjään tai mielenkiinnon kohteitaan suoramarkkinointia varten. Rekisteröidylle tulee ilmoittaa profiloinnista, jos sitä hyödynnetään rekisteröidyn henkilötietojen käsittelyssä ja analysoinnissa.

Pseudonymisoinnissa henkilötietoja muutetaan siten, että niitä ei pysty täsmällisesti yhdistämään kehenkään henkilöön. Pseudonymisointi eroaa anonymisoinnista siten, että muutetut tiedot voi tarvittaessa palauttaa alkuperäiseen muotoonsa ja yhdistää ne henkilöön kenen tietoja muutettiin. Pseudonymisoituihin tietoihin sovelletaan tietosuojasäännöksiä palautettavuutensa takia.

Rajat ylittävällä käsittelyllä tarkoitetaan henkiötietojen siirtoa EU/ETA-alueen ulkopuolelle sekä henkilötietojen käsittelyä, joka tapahtuu useammassa kuin yhdessä valtiossa. Rajat ylittävää käsittelyä on esimerkiksi se, kun rekisterinpitäjä käsittelee tietoja vähintään kahdessa toimipaikassa eri valtioissa. Rajat ylittäväksi käsittelyksi katsotaan myös se, kun käsittely tapahtuu yhden valtion sisällä, mutta vaikuttaa useammassa kuin yhdessä valtiossa oleviin rekisteröityihin.

Rekisterillä tarkoitetaan mitä tahansa henkilötietoja sisältävää tietojoukkoa, mistä tiedot ovat saatavilla tietyin perustein. Rekisteriä voidaan ylläpitää esimerkiksi tietoteknisesti tietokoneella tai perinteisesti paperilla arkistoissa. Henkilörekistereitä voivat olla esimerkiksi jäsen-, käyttäjä- ja asiakasrekisterit sekä osallistujaluettelot.

Rekisterinpitäjä voi olla yritys, yhdistys, sairaala, koulu, verkkokauppa, yksityishenkilö, viranomainen tai muu taho, joka käsittelee henkilötietoja. Rekisterinpitäjän velvollisuuksiin kuuluu suunnitella ja valvoa henkilötietojen käsittelyä sekä määritellä miksi ja miten henkilötietoja kerätään ja säilytetään. Rekisterinpitäjä on aina lopullisessa vastuussa henkilötietojen käsittelystä, mutta rekisterinpitäjä voi käyttää toimessaan apuna ulkopuolista henkilötietojen käsittelijää esimerkiksi tietojen teknistä säilyttämistä varten. Rekisterinpitäjän tehtäviin kuuluu myös tietosuojaselosteen tekeminen.

Rekisteröidyksi kutsutaan henkilöä, kenen henkilötietoja rekisterinpitäjä käsittelee. Rekisteröidyllä on yleisen tietosuoja-asetuksen mukaan monia oikeuksia, kuten oikeus tarkastaa mitä tietoja rekisterinpitäjä on kerännyt hänestä.

Suostumuksella tarkoitetaan rekisteröidyn hyväksyntää henkilötietojensa käsittelylle. Suostumuksen tulee olla aidosti vapaaehtoinen ja sen antamisesta on myös pystyttävä kieltäytymään. Suostumusta tulee kysyä henkilötietoja kerättäessä, jotta rekisteröidyllä on mahdollisuus harkita mitä tietoja hän on valmis jakamaan.

Tietojenkäsittelysopimus tai henkilötietojen käsittelysopimus (data processing agreement, DPA) tehdään silloin kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta tai lukuun. Sopimuksessa täytyy kuvata muun muassa henkilötietojen käsittelyn kesto, käsittelyn luonne ja tarkoitus, mitä henkilötietoja käsitellään sekä rekisterinpitäjän velvollisuudet ja oikeudet. Henkilötietojen käsittelijä toimii aina rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Rekisterinpitäjä voi antaa nämä ohjeet tietojenkäsittelysopimuksessa.

Tietosuojaseloste on kirjallinen kuvaus siitä, kuinka rekisterinpitäjä käsittelee henkilötietoja. Tietosuojaselosteen tulee vastata muun muassa esimerkiksi siihen, mihin tarkoituksiin organisaatio käyttää pyytämiään tietoja, kuinka kauan rekisteröidyn tietoja säilytetään ja minkälaiset oikeudet rekisteröidyllä on.

Tietosuojavaltuutettu ja tietosuojavaltuutetun toimisto toimii kansallisena tietosuojaviranomaisena Suomessa. Tietosuojaviranomaisella on oikeus muun muassa tutkia rekisterinpitäjän henkilötietojen käsittelyä sekä pyrkiä toimillaan korjaamaan puutteellisia henkilötietojen käsittelyyn liittyviä käytänteitä. Tietosuojaviranomainen voi antaa ohjeita, varoituksia, määräyksiä tai huomautuksia sekä määrätä hallinnollisia seuraamusmaksuja, eli sakkoja.

Tietosuojavastaava on organisaation, kuten esimerkiksi kunnan tai yrityksen sisäinen asiantuntija tietosuojaan liittyvissä asioissa. Tietosuojavastaava huolehtii siitä, että organisaation koko henkilöstö johtoa myöten noudattaa tietosuojasäännöksiä, ja tarvittaessa myös ohjeistaa heitä tietosuojaan liittyvissä ongelmatilanteissa. Jos organisaatiossa käsitellään arkaluontoisia henkilötietoja laajamittaisesti tai seurataan ihmisten toimintaa, on tietosuojavastaava nimitettävä.

Tietoturva on yksi niistä menetelmistä, jolla organisaatioissa varmistetaan tietosuojan toteutuminen. Tietoturvan avulla suojataan teknisesti tietoaineistot ja tietojärjestelmät, joissa esimerkiksi rekisteröityjen tietoja säilytetään. Asianmukaisella tietoturvalla varmistetaan tietojen saatavuus, eheys, käytettävyys, luottamuksellisuus ja rekisteröidyn oikeuksien toteutuminen.

Tietoturvaloukkauksella tarkoitetaan tilannetta, jossa henkilötietoja häviää, tiedot muuttuvat tai tietoja päätyy henkilöille, joilla ei pitäisi olla oikeutta niihin. Tietoturvaloukkaus voi liittyä tietomurtoihin tai hakkerointiin, mutta myös esimerkiksi muistitikun, puhelimen tai salasanojen häviäminen ovat tietoturvaloukkauksia.

Yhteisrekisterinpitäjäksi kutsutaan rekisterinpitäjiä, jotka määrittelevät keskenään henkilötietojen käsittelyn tarkoituksen ja keinot. Yhteisrekisterinpitäjiä tulee olla vähintään kaksi, mutta niitä voi olla myös useampia. Yhteisrekisterinpitäjien täytyy myös sopia keskenään kunkin yhteisrekisterinpitäjän vastuut ja toimet henkilötietojen suojaamiseksi.

Vaikutustenarviointi (data protection impact assessment, DPIA) on menettely, jonka tarkoituksena on tutkia ja tunnistaa tietosuojan toteutumiseen liittyviä riskejä ja uhkia suhteessa hyötyihin ja rekisteröidyn oikeuksiin. Vaikutustenarvioinnin avulla voidaan pohtia mitä toimenpiteitä ja päätöksiä kannattaa tehdä organisaatiossa, jotta rekisteröityjen henkilötietojen käsittely olisi mahdollisimman turvallista ja tietosuoja-asetusten mukaisia.

02
Tietosuojan perusteet

2.1 Tietosuojaperiaatteet

Yleisessä tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyn periaatteista, joiden tarkoituksena on ohjata organisaatioiden tietojen käsittelyä. Tietosuojaperiaatteet siis neuvovat mitä tietoja on hyväksyttyä käsitellä ja miten.

Käyttötarkoitus sidonnaisuus

Käyttötarkoitussidonnaisuus tarkoittaa sitä, että organisaation on **kerättävä** henkilötietoja vain tiettyä **ennalta määriteltyä asiaa** tai tehtävää **varten**. Organisaatio ei saa käyttää kerättyjä henkilötietoja myöhemmin muuhun tarkoitukseen, kuin mitä varten tiedot oli alun perin kerätty. Henkilötietoja voidaan kerätä esimerkiksi suoramarkkinointia ja asiakassuhteiden hoitoa varten.

Tietojen minimointi

Tietojen minimointi tarkoittaa sitä, että rekisteröidyltä kerättävät ja käsiteltävät **henkilötiedot tulee pitää minimissään**. Tämä edellyttää, että organisaatio määrittelee henkilötietojen käsittelyn tarkoituksen, huolehtii säilytettävien henkilötietojen päivittämisestä sekä poistaa tarpeettomat ja virheelliset tiedot säännöllisesti. Tietojen säilytysaika tulee pitää myös niin lyhyenä kuin mahdollista, eikä tietoja saa säilyttää varmuuden vuoksi myöhempää käyttöä varten, ellei säilytykselle ole esimerkiksi lakiin perustuvaa velvoitetta tai muuta syytä.

Tietojen täsmällisyys

Tietojen täsmällisyys tarkoittaa sitä, että käsiteltävien **henkilötietojen tulee olla virheettömiä ja ajantasaisia**. Organisaation täytyy huolehtia tietojen säännöllisestä tarkastamisesta ja sen tulee korjata tai poistaa väärät tiedot tarpeen tullen. Mikäli organisaatio on jakanut asiakkaan henkilötietoja muille tahoille, muutoksista ja korjauksista täytyy ilmoittaa myös heille.

Tietojen säilytyksen rajoittaminen

Tietojen säilytyksen rajoittamisella tarkoitetaan sitä, että henkilötietoja tulee **säilyttää** organisaatiossa vain **niin kauan** kuin **henkilötiedot** ovat **tarpeellisia**. Organisaation tulee esimerkiksi asiakassuhteen loppuessa päättää, ovatko asiakkaan tiedot organisaatiolle vielä tarpeellisia, vai olisiko ne aiheellista poistaa. Tarpeellisia syitä henkilötietojen säilyttämiselle voi olla esimerkiksi laskutus, perintä, oikeudelliset perusteet, reklamaatio tai takuu.

Tietojen eheys ja luottamuksellisuus

Tietojen eheys ja luottamuksellisuus tarkoittaa sitä, että henkilötietoja **käsitellään turvallisesti** ja siten, että ulkopuolisilla ei ole pääsyä tietoihin. Organisaation tulee huolehtia turvallisuuden takaamiseksi tarpeellisten suojatoimien, kuten riskien, tietosuoja- ja tietoturvaohjeistuksen riittävyyden ja henkilötietojen teknisen suojauksen arvioimisesta.

Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja tulee käsitellä **yleistä tietosuoja-asetusta** ja muita henkilötietojen käsittelyä koskevia kansallisia lakeja **kunnioittaen**. Henkilötietojen käsittelyn on myös pohjauduttava lailliseen perusteeseen, kuten oikeutettuun etuun. **Läpinäkyvyydellä** tarkoitetaan sitä, että rekisteröidylle tulisi kertoa ymmärrettävästi miten ja mitä varten hänen henkilötietojaan kerätään. **Kohtuullisuudella** tarkoitetaan sitä, että rekisterinpitäjä ottaa henkilötietojen käsittelyssä huomioon rekisteröidyn edun ja käyttää tietoja vain siihen tarkoitukseen mitä varten rekisteröity on luovuttanut tietonsa

Rekisterinpitäjän osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa sitä, että organisaation on pystyttävä **näyttämään**, että **tietosuojalainsäädäntöä noudatetaan** kaikissa henkilötietojen käsittelyn vaiheissa. Rekisterinpitäjän tulee siis dokumentoida henkilötietojen käsittelyyn liittyvät tavat muun muassa henkilöstön tietosuojakoulutuksista ja salasanapolitiikasta, jotta se voi jälkikäteen osoittaa noudattaneensa tietosuojaperiaatteita esimerkiksi tietoturvaloukkauksen sattuessa.

2.2 Henkilötietojen käsittelyn peruste

Henkilötietojen käsittely on yleisen tietosuoja-asetuksen mukaan hyväksyttyä, mikäli se perustuu johonkin tässä osiossa esiteltyihin käsittelyperusteisiin, kuten esimerkiksi rekisteröidyn suostumukseen.

Käsittelyperuste täytyy määritellä esimerkiksi ennen rekisteröidyn henkilötietojen keräämistä suoramarkkinointia varten, koska perustetta ei voi myöhemmin muuttaa toiseksi.

Rekisteröidyn suostumus

Rekisteröidyn suostumuksen henkilötietojensa käsittelylle tulee olla vapaaehtoinen, yksilöity ja tietoisesti tehty. Suostumusta tulee kysyä rekisteröidyltä erikseen jokaista ennalta määriteltyä henkilötietojen käyttötarkoitusta varten. Suostumus pitää olla myös helposti peruutettavissa.

Vaikeneminen, esitäytetty rasti ruudussa tai jonkin asian tekemisen välistä jättäminen ei ole suostumuksen antamista. Mikäli organisaatio käsittelee arkaluontoisia henkilötietoja, siirtää henkilötietoja kolmansiin maihin tai tekee tiedoille automatisoituja yksittäispäätöksiä, täytyy rekisterinpitäjän pyytää tähän rekisteröidyltä nimenomainen suostumus.

Sopimus

Sopimukseen perustuva henkilötietojen käsittely on tarpeen silloin kun se tarvitaan sopimuksen täytäntöön panemiseksi. Esimerkki sopimukseen perustuvasta henkilötietojen käsittelystä on tilanne, jossa verkkokauppa käsittelee asiakkaan tietoja toimittaakseen tehdyn tilauksen perille.

Lakisääteinen velvoite

Henkilötietojen käsittely voi perustua rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseen, jolloin peruste käsittelylle löytyy Suomen kansallisesta lainsäädännöstä tai Euroopan Unionin lainsäädännöstä. Esimerkki lakisääteisestä velvoitteesta on työnantajan velvoite kertoa työntekijänsä palkkatiedoista veroviranomaisille.

Elintärkeiden etujen suojaaminen

Silloin kun rekisteröity tai muu henkilö on vaarassa, on henkilötietojen käsittely hyväksyttyä elintärkeiden etujen suojaamiseksi. Elintärkeiden etujen turvaamiseen liittyvät tilanteet voivat olla esimerkiksi olosuhteita, joissa henkilön fyysisen koskemattomuus on vaarantunut tai on kyse elämästä ja kuolemasta (luonnonkatastrofi tai epidemia).

Yleinen etu ja julkinen valta

Henkilötietojen käsittely on sallittua tilanteissa, joissa yleinen etu tai organisaation julkinen valta sallii käsittelyn lain puitteissa. Muun muassa viranomaisten suorittamat suunnittelu- ja selvitystehtävät ja sukututkimukset ovat esimerkkejä olosuhteista, joissa yleinen etu ja julkinen valta toimii käsittelyperusteena.

Oikeutettu etu

Oikeutettua etua voidaan käyttää käsittelyperusteena esimerkiksi silloin kun rekisteröidyn ja rekisterinpitäjän välillä on jokin merkitsevä suhde, kuten asiakas- tai työsuhde. Oikeutetun edun tilanteita ovat esimerkiksi kaupan tallentava valvontakamera omaisuuden suojaamiseksi tai henkilötietojen siirtäminen uuteen järjestelmään konsernin sisällä.

Erityisten henkilötieto-ryhmien käsittely

Erityisiä henkilötietoryhmiä eli arkaluontoisia tietoja, kuten ammattiliiton jäsenyyttä tai terveyttä koskevia tietoja, ei pääsääntöisesti saa käsitellä ollenkaan, ellei käsittelyyn ole olemassa jokin hyväksyttävä peruste, kuten tietosuoja-asetuksessa sallittu poikkeus tai muu laillinen peruste. Rekisteröidyn nimenomaisella suostumuksella rekisterinpitäjä voi käsitellä arkaluontoisia henkilötietoja yhtä tai useampaa käyttötarkoitusta varten, ellei lainsäädäntö estä tätä yksiselitteisesti.

Mikäli asiakkaiden arkaluontoisten henkilötietojen käsittely on tarpeellista organisaatiossa, niin tietojen käsittelyyn ja säilyttämiseen tulee pyytää asiakkaiden **suostumus**. Ongelmia voi syntyä silloin kun joistakin tiedoista voi välillisesti käydä ilmi asiakkaan arkaluontoisia tietoja. Esimerkiksi erityisruokavaliosta voi päätellä henkilön terveydentilaan liittyviä tietoja.

Jos tällaisia tietoja tallennetaan pysyvästi asiakasrekisteriin, kannattaa tähän ehdottomasti pyytää rekisteröidyltä suostumus. Mikäli yrityksessä käsitellään arkaluontoisia tietoja, joiden käsittelyyn ei ole asiakkailta lupaa, ne pitää poistaa välittömästi tai pyytää rekisteröidyiltä lupa jälkikäteen.

Terveysteknologia yhtiöt käyttävät markkinointimateriaalissaan usein potilaskuvia, jotka luokitellaan arkaluontoisiksi henkilötiedoiksi.

2.3 Rekisteröidyn oikeudet

Yleisen tietosuoja-asetuksen ydinideana on, että jokaisella yksilöllä on oikeus omien henkilötietojensa hallintaan, suojaamiseen ja turvalliseen sekä lainmukaiseen käsittelyyn.

Tietojen keräämisen yhteydessä rekisteröidylle eli asiakkaalle tulee kertoa hänen oikeuksistaan esimerkiksi **tietosuojaselosteen** avulla.

Oikeus saada tietoa henkilötietojen käsittelystä

Henkilötietojen käsittelyn tulee olla läpinäkyvää. Tämän vuoksi rekisteröidyllä on oikeus saada tietää, kuinka hänestä kerätään tietoja ja miten niitä käsitellään.

Rekisteröidylle täytyy kertoa esimerkiksi rekisterinpitäjän yhteystiedot, käsittelyn tarkoitukset, tietojen käsittelyperuste, tietojen käsittelyajoista, luovutetaanko tai siirretäänkö tietoja EU:n ja ETA-alueen ulkopuolelle, rekisteröidyn oikeuksista sekä mistä tiedot on saatu, jos ne on saatu muualta kuin rekisteröidyltä.

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan kaikki tiedot hänestä, ja ”tulla unohdetuksi”. Tietojen poistamisesta tulee ilmoittaa myös jokaiselle taholle, jolle rekisteröidyn tietoja on luovutettu.

Rekisteröidyn tiedot pitää poistaa muun muassa silloin kun henkilötietoja ei enää tarvita sitä tarkoitusta varten minkä vuoksi ne alun perin kerättiin, rekisteröity peruuttaa suostumuksensa tietojen käsittelyn perusteesta, rekisteröity ei halua tietojaan käytettävän suoramarkkinointiin tai henkilötietojen käsittelylle ei ole lainmukaista perustetta.

Oikeus oikaista tietoja

Rekisteröidyllä on oikeus vaatia rekisterinpitäjältä oikaisua virheellisiin tietoihin sekä täydennystä puutteellisiin henkilötietoihin. Oikaisupyynnön tekeminen on lähtökohtaisesti aina maksutonta. Mikäli pyyntö on kohtuuton tai perusteeton, voi rekisterinpitäjä periä kohtuullisen maksun oikaisun suorittamisesta tai kieltäytyä oikaisun toteuttamisesta. Rekisterinpitäjän tulee ilmoittaa henkilötietojen oikaisuista jokaiselle taholle, kelle rekisteröidyn tietoja on luovutettu.

Oikeus saada tutustua tietoihin

Rekisteröidyllä on oikeus saada tietää mitä tietoja rekisterinpitäjällä on hänestä kerättynä. Rekisteröity voi halutessaan pyytää rekisterinpitäjää lähettämään kaikki hänestä kerätyt tiedot itselleen.

Jos rekisteröity tekee pyynnön sähköisesti, rekisterinpitäjän tulee toimittaa tiedot rekisteröidylle sähköisesti, ellei rekisteröity erikseen pyydä toista toimitusmuotoa tiedoille.

Oikeus olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon, kuten profiloinnin, kohteeksi. Rekisteröity voi myös vaatia, että häntä koskevat päätökset tekee ihminen esimerkiksi tilanteissa, joilla voi olla rekisteröidyn kannalta oikeudellisia vaikutuksia.

Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä henkilökohtaisiin syihin vedoten silloin kun tietoja käsitellään esimerkiksi yleistä etua koskevan asian saavuttamiseksi tai rekisterinpitäjän tai kolmansien osapuolten oikeutettujen etujen toteuttamiseksi.

Rekisterinpitäjän täytyy lopettaa tietojen käsittely, ellei se pysty perustelemaan hyvällä syyllä miksi käsittely syrjäyttäisi rekisteröidyn edut, oikeudet ja vapaudet.

Rekisteröity voi vastustaa henkilötietojensa käyttöä suoramarkkinointiin ilman perusteluja, jolloin se tulee lopettaa.

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada rekisterinpitäjälle antamansa henkilötiedot takaisin ja siirtää tiedot toiselle rekisterinpitäjälle. Rekisteröidyllä on myös oikeus vaatia rekisterinpitäjää siirtämään kyseiset tiedot toiselle rekisterinpitäjälle suoraan, jos se on teknisesti mahdollista.

Rekisteröity voi käyttää oikeutta tietojen siirtoon järjestelmästä toiseen silloin kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen.

Henkilötietoja vastaanottavan uuden rekisterinpitäjän tulee varmistaa, että toiselta rekisterinpitäjältä saadut tiedot ovat tarpeellisia sen käyttötarkoituksia varten. Mikäli näin ei ole, pitää tarpeettomat tiedot poistaa ja jättää käsittelemättä.

Oikeus rajoittaa tietojen käsittelyä

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää rajoittamaan henkilötietojensa käsittelyä. Rekisteröidyllä on oikeus vaatia tietojensa käsittelyn rajoittamista esimerkiksi silloin kun hän kiistää henkilötietojensa paikkansapitävyyden tai pitää tietojensa käsittelyä lainvastaistaisena.

Rekisteröidyn henkilötietojen käsittelyä voidaan rajoittaa esimerkiksi poistamalla hänen tietonsa julkiselta verkkosivulta.

Rekisteröidyn oikeuksien käyttäminen

Rekisteröidyn pyyntöihin oikeuksiensa käyttämisestä tulee vastata ilman viivytystä enintään kuukauden määräajan kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan pidentää, mikäli rekisterinpitäjä pystyy perustelemaan rekisteröidylle, miksi se tarvitsee lisää aikaa pyynnön toteuttamiseen.

Jos rekisterinpitäjä kieltäytyy rekisteröidyn pyynnöstä, tästä tulee ilmoittaa rekisteröidylle kuukauden kuluessa pyynnöstä.

Mikäli rekisterinpitäjä epäilee pyynnön tehneen rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää sopivaksi katsomallaan tavalla rekisteröityä varmistamaan henkilöllisyytensä.

Rekisterinpitäjä voi kieltäytyä toteuttamasta rekisteröidyn oikeuksia esimerkiksi jos rekisteröidyn pyynnöt ovat toistuvia ja perusteettomia tai ne voisivat uhata yleistä turvallisuutta.

2.4 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjä on aina viime kädessä vastuussa tietosuojalainsäädännön toteutumisesta sen omassa toiminnassa, sekä henkilötietojen käsittelijöiden toiminnassa.

Mikäli rekisterinpitäjä hyödyntää asiakastapahtumassa ulkopuolisia **henkilötietojen käsittelijöitä**, kuten valokuvaajaa tai catering-palvelua, täytyy heidän käsitellä henkilötietoja rekisterinpitäjän antamien ohjeiden mukaisesti. Heidän kanssaan tulee myös laatia sopimus, josta selviää osapuolten velvollisuudet liittyen henkilötietojen käsittelyyn. Jos henkilötietojen käsittelijä haluaa käyttää apunaan muita käsittelijöitä, tähän täytyy saada kirjallinen lupa rekisterinpitäjältä.

Rekisterinpitäjän kuuluu myös huolehtia organisaation teknisistä ja organisatorisista toimenpiteistä, kuten tietoturvasta, joilla varmistetaan henkilötietojen turvallinen käsittely.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet

Sisäänrakennetulla ja oletusarvoisella tietosuojalla (privacy by design ja privacy by default) tarkoitetaan näkökulmaa, jossa tietosuojan periaatteiden toteutuminen huomioidaan organisaation palvelun, sovelluksen tai tapahtuman koko elinkaaren ajaksi aina alun suunnitteluvaiheesta tietojen poistamiseen saakka.

Tietosuojan huomioiminen ei ole pelkästään esimerkiksi tietosuojavastaavan vastuulla, vaan kaikkien henkilöiden, joiden työhön liittyy henkilötietojen käsittelyä tai käsittelyn suunnittelua.

Yhteisrekisterinpitäjyys

Yhteisrekisterinpitäjyydessä, kahden tai useamman organisaation tulee yhdessä määritellä omat vastuualueensa henkilötietojen käsittelystä sekä rekisteröityjen oikeuksien toteuttamisesta ja tiedottamisesta. Yhteisrekisterinpitäjien roolit tulee olla rekisteröityjen saatavilla esimerkiksi tietosuojaselosteen muodossa.

2.5 Tietosuojavastaava ja tietoturvaloukkaus

Tietosuojavastaavan tehtävänä on valvoa, että organisaatiossa henkilötietoja käsitellään tietosuojasäädösten vaatimalla tavalla. Tietosuojavastaava on myös henkilö, kehen rekisteröidyt ja organisaation työntekijät voivat olla yhteydessä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietosuojavastaavan tehtäviin kuuluu työntekijöiden ja johdon ohjeistaminen, neuvonta ja kouluttaminen tietosuojaan liittyvissä asioissa organisaation sisällä. Tietosuojavastaava tulee nimittää silloin kun organisaatio käsittelee henkilötietoja laajamittaisesti, säännöllisesti ja järjestelmällisesti tai käsittely kohdistuu erityisiin henkilötietoryhmiin.

Henkilötietojen tietoturvaloukkauksesta on kyse silloin kun henkilötietoja häviää, tiedot muuttuvat tai tietoja päätyy henkilöille, joilla ei pitäisi olla oikeutta niihin.

Tietoturvaloukkauksia ovat esimerkiksi muistitikun tai työpuhelimen hukkaaminen tai suoramarkkinointiviestin lähettäminen sähköpostilla niin, että sen vastaanottajat voivat nähdä muiden sähköpostin saaneiden sähköpostiosoitteet. Myös tietomurrot, haittaohjelmatartunnat sekä henkilötietoja sisältävien tulosteiden unohtaminen tulostimeen muiden saataville ovat tietoturvaloukkauksia.

Ilmoita tietoturvaloukkauksista

Mikäli organisaation työntekijä, palveluntarjoaja tai asiakas epäilee, että henkilötietojen käsittely ei ole täysin turvallista tai rekisteröityjen oikeudet ovat vaarantuneet, on heidän hyvä ilmoittaa havainnostaan rekisterinpitäjälle.

Jos tietoturvaloukkaus asettaa yksilön oikeudet ja vapaudet vaaraan, pitää rekisterinpitäjän ilmoittaa loukkauksesta tietosuojavaltuutetulle mahdollisimman pian ja viimeistään 72 tuntia loukkauksen havaitsemisesta.

Jokainen työntekijä on velvollinen ilmoittamaan tietosuojaan liittyvistä epäkohdista tai epäilyistä joko esihenkilöllensä tai suoraan tietosuojavastaavalle.

Tietoturvaloukkauksen seuraukset

Tietoturvaloukkausta epäiltäessä tietosuojavaltuutettu voi pyrkiä muokkaamaan organisaation henkilötietojen käsittelyä tietosuojalainsäädännön mukaiseksi erilaisin keinoin.

Tietosuojavaltuutettu voi korjaavana toimina esimerkiksi varoittaa rekisterinpitäjää kyseenalaisista aiotuista käsittelytoimista, antaa huomautuksen vääränlaisista käsittelytoimista, määrätä organisaatio ilmoittamaan tietoturvaloukkauksesta rekisteröidyille, asettaa väliaikaisen tai pysyvän henkilötietojen käsittelykiellon, määrätä hallinnollisen seuraamusmaksun tai määrätä tiedonsiirron keskeyttämisestä kolmannessa maassa sijaitsevaan organisaatioon.

Jos jokin epäilyttää henkilötietojen käsittelyssä, niin älä epäröi olla yhteydessä organisaation tietosuojavastaavaan.

03

Tietosuojaohjeita tapahtumiin

3.1 Tietosuojaroolit, sopimukset ja selosteet

Silloin kun organisaatio järjestää tapahtuman **yksin**, on se vastuussa tapahtumaan osallistuvien asiakkaiden ja henkilöiden henkilötiedoista. Organisaatio on vastuussa myös tapahtumaa tukevien yritysten henkilötietojen käsittelystä, jonka vuoksi näiden yritysten kanssa täytyy tehdä **tietojenkäsittelysopimus**.

Tyypillisiä henkilötietojen käsittelijöitä tapahtumissa ovat muun muassa catering-palvelut, viestintätoimistot, valokuvaajat, etäkokousjärjestelmät ja muut yritykset, joiden kanssa jaetaan henkilötietoja. Esimerkiksi catering-palvelujen kokeille voi joutua kertomaan erityisruokavaliota noudattavien ihmisten nimet, jolloin tietojenkäsittelysopimus on tehtävä.

Tietojenkäsittelysopimuksessa kannattaa sopia ulkopuolisen henkilötietojen käsittelijän kanssa vahingonkorvallisuus-velvollisuudesta rekisterinpitäjälle, mikäli ulkopuolisen henkilötietojen käsittelijän toimista syntyisi vahinkoa rekisteröidyille.

Mikäli organisaatio järjestää tapahtuman **yhteistyössä** muiden yritysten kanssa **ilman yhteisrekisterinpitäjyyttä**, ovat kaikki yritykset itsenäisiä rekisterinpitäjiä.

Ilman yhteisrekisterinpitäjyyttä jokainen tapahtumaan järjestämiseen osallistuva yritys määrittää itsenäisesti henkilötietojen käsittelyä koskevat sopimuksensa henkilötietoja käsittelevien yritysten kanssa. Jokainen yritys joutuu myös pyytämään suostumusta erikseen henkilötietojen käsittelyä varten tapahtumaan osallistuvilta henkilöiltä.

Organisaation järjestäessä tapahtuman **yhdessä yhden tai useamman** yrityksen kanssa siten, että ne sopivat keskenään henkilötietojen käsittelyn tarkoitukset ja keinot, on kyseessä **yhteisrekisterinpitäjyys**. Tällöin yritykset yhdessä määrittelevät ja sopivat henkilötietojen käsittelyä koskevat seikat yhteiseen sopimukseen esimerkiksi henkilötietoja käsittelevien tukiyritysten ja asiakkailta kerättävien tietojen osalta.

Yhteisrekisterinpitäjyydestä sovitaan kirjallisesti jokaisen rekisterinpitäjän, eli tapahtumaa järjestämässä olevan yrityksen kanssa. Yhteisrekisterinpitäjyys päättyy, kun henkilötietojen käsittelyn tarkoitus päättyy.

Tietosuojaseloste

Kaikilla yrityksillä, jotka keräävät työntekijöistään tai asiakkaistaan tietoja on tietosuojaselosteen laatimisvelvollisuus. Asiakastapahtumia järjestettäessä henkilötietojen keräämiseltä harvemmin voi välttyä, joten asiakastapahtuman järjestävän organisaation tulee laatia asianmukainen tietosuojaseloste.

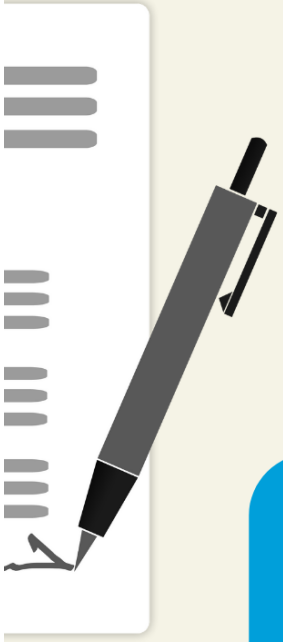
Tietosuojaselosteessa rekisteröidyille, eli asiakkaille kerrotaan mitä henkilötietoja heistä kerätään, miksi ja millaisin perustein. Tietosuojaselosteen tulee olla tiivis, selkeä ja mahdollisimman helposti ymmärrettävällä kielellä kirjoitettu.

Tietosuojaselosteita voi laatia erikseen erilaisia käyttötarkoituksia varten, esimerkiksi organisaation työntekijöille, tapahtumille ja asiakkaille on mahdollista laatia omat tietosuojaselosteensa.

Tietosuojaselosteen tiedot täytyy toimittaa rekisteröidylle silloin kun häneltä kerätään tietoja, tai selosteen täytyy jollain muulla tavoin olla helposti saatavilla. Tietosuojaselosteeseen ohjaavan linkin voi laittaa näkyville muun muassa yrityksen kotisivuille, yhteydenotto- ja rekisteröintilomakkeisiin, uutiskirjeisiin tai sähköpostimarkkinointiviesteihin

Tietosuojaseloste sisältää...

- Rekisterinpitäjän yhteystiedot
- Tietosuojavastaavan yhteystiedot
- Henkilötietojen käsittelyn tarkoitukset sekä käsittelyperuste, kuten esimerkiksi oikeutettu etu, sopimus tai suostumus
- Kyseessä olevat henkilötietoryhmät
- Henkilötietojen vastaanottajat tai vastaanottajaryhmät
- Tiedot tietojen siirrosta kolmansiin maihin
- Henkilötietojen säilyttämisaika
- Rekisteröidyn oikeudet, kuten oikeus tietojen poistamiseen
- Jos käsittely perustuu suostumukseen, tieto oikeudesta peruuttaa suostumus milloin tahansa
- Oikeus tehdä valitus valvontaviranomaiselle
- Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus ja tieto siitä onko rekisteröidylle mahdollisia seurauksia tietojen antamatta jättämisestä
- Mistä henkilötiedot on saatu?
- Mahdolliset tiedot automaattisesta päätöksenteosta (kuten profiloinnista) ja merkittävyydestä rekisteröidyn kannalta



Tietojenkäsittelysopimus

Yleisen tietosuoja-asetuksen mukaan organisaation tulee tehdä kirjallinen yhteistyösopimus, kuten tietojenkäsittelysopimus, yrityksen kanssa, joka käsittelee henkilötietoja sen puolesta.

Esimerkiksi suoramarkkinointikirjeiden postitus saatetaan ulkoistaa sitä tarjoavalle yhteistyökumppanille tai arpajaisten järjestäminen sen osaavalle mainostoimistolle.

Ulkopuolinen yritys ei saa käyttää toisen henkilötietojen käsittelijän apua ilman rekisterinpitäjän lupaa tai poiketa rekisterinpitäjän antamista ohjeista itsenäisesti, joista on sovittu esimerkiksi tietojenkäsittelysopimuksessa.

Tietojenkäsittelysopimuksessa on hyvä sopia muun muassa

Tietojen käsittelyn tarkoitus: Selitetään, mihin tarkoitukseen tietoja käsitellään.

Käsittelyn kesto ja luonne: Määritellään, kuinka kauan tietoja käsitellään ja millä tavalla niitä käsitellään.

Tietojen luovuttaminen: Sopimuksessa voidaan määritellä, saako käsittelijä luovuttaa tietoja kolmansille osapuolille tai toisille käsittelijöille.

Tietoturva: Sovitaan toimenpiteistä, joilla varmistetaan tietojen asianmukainen suojaaminen.

Käsittelijän velvollisuudet: Selvitetään, mitä velvollisuuksia käsittelijällä on tietojen käsittelyssä.

Rekisterinpitäjän velvollisuudet: Määritellään rekisterinpitäjän vastuut ja velvollisuudet tietojen luovutuksen yhteydessä.

Auditoinnit: Sovitaan mahdolliset säännöt sille, onko rekisterinpitäjällä oikeus tarkistaa käsittelijän tietoturvakäytännöt.

3.2 Henkilötietojen kerääminen ja säilyttäminen

Yleisessä tietosuoja-asetuksessa ei ole tiettyjä säädöksiä siitä, mitä tietoja asiakkaista tai potentiaalisista asiakkaista saa tallentaa, vaan asioita käsitellään yleisemmin pelkän rekisteröidyn kannalta. Siksi organisaation täytyy noudattaa **tietosuojaperiaatteita** asiakastietojen keräämisessä ja kerätä heistä vain aidosti tarpeellisia ja asianmukaisia tietoja.

Asiakkaiden tietoja saa säilyttää asiakasrekisterissä niin kauan kuin rekisteröidyn ja organisaation välillä on olemassa jonkinlainen asianmukainen yhteys tai sopimussuhde, kuten kestosopimus.

Asiakkaan ostaessa kertaluontoisesti jotain, hänen henkilötietoja saa käsitellä asiakasrekisterissä vielä kohtuullisen ajan verran. Tämä mahdollistaa edelleen joksikin aikaa asiakasviestinnän ja suoramarkkinoinnin henkilölle. **Asiakasrekisterissä** on mahdollista käsitellä laajempia tietoja henkilöstä kuin potentiaalisten asiakkaiden suoramarkkinointirekisterissä.

Suomessa asianmukaisen yhteyden päättymisen jälkeen kohtuullisena pidettyä henkilötietojen säilytysaikana on pidetty jopa 3-4 vuotta. **Erityislainsäädäntö** saattaa vaikuttaa asianmukaisen yhteyden kestoon. Siksi esimerkiksi **perinnän** ja **takuun** voimassaolon ajan asianmukainen yhteys jatkuu ja tietojen säilyttäminen voi olla mahdollista pitkäänkin.

Yleisen tietosuoja-asetuksen mukaan oikeutettu etu sopii alustavaksi perusteeksi potentiaalisten asiakkaiden suoramarkkinointirekisterien ylläpitämiselle. **Suoramarkkinointirekistereihin** saa kerätä tietoja myös rekisteröidyn suostumukseen perustuen tai muulla laillisella tavalla.

B2B -markkinointirekistereihin voi kerätä tietoja, jotka ovat olennaisia käyttötarkoitustaan varten. Kerättävien tietojen tulisi koskea esimerkiksi potentiaalisen yritysasiakkaan yhteyshenkilön asemaa, yhteystietoja ja muita henkilön työhön liittyviä tehtäviä.

Pelkkä markkinointiarpajaisiin osallistuminen ei lähtökohtaisesti riitä perusteeksi henkilön tietojen tallettamiseen asiakasrekisteriin, vaan korkeintaan potentiaalisten asiakkaiden rekistereihin.

3.3 IBA ja profilointi

IBA (Interest-Based Advertising) tarkoittaa internetin käyttäjän nettikäyttäytymisestä, evästeistä ja sijaintitiedoista kerättyjen tietojen hyödyntämistä henkilölle kohdennetussa mainonnassa toisiinsa liittymättömillä verkkosivuilla, sovelluksissa tai somessa. **Nettikäyttäytyminen** voi olla esimerkiksi tiettyjen tuotteiden selaamista verkkokaupassa tai hakukoneen käyttämistä.

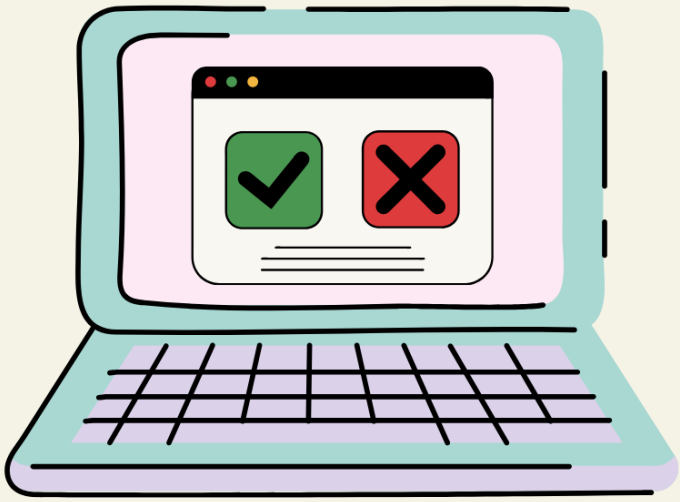
IBA-mainontaa hyödyntävien osapuolien on tärkeää olla **avoimia** kuluttajan tietojen keräämisestä ja kohdennettujen mainosten käyttämisestä. Kolmannen osapuolen ja verkko-operaattorin täytyy ilmoittaa verkkosivuillaan selkeästi IBA-mainontaan liittyvät omat käytännöt esimerkiksi laitteiden välisestä seurannasta sekä kuvaukset tiedoista, joita kerätään, tiedonkeräämisen tarkoitukset ja mitkä verkkosivut ja sovellukset saavat tietoja haltuunsa.

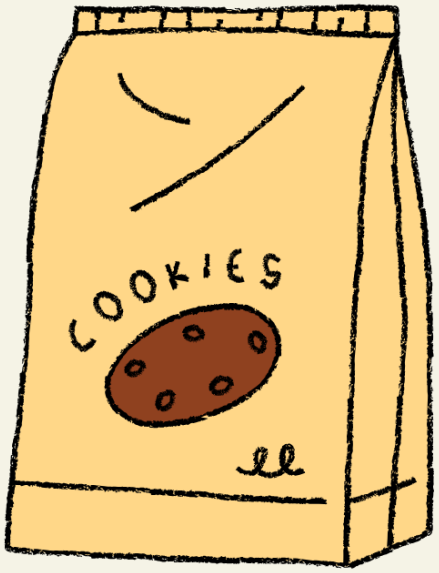
Reaaliaikaista mainosta varten kerättyjä tarkkoja sijaintitietoja saa säilyttää vain keräämishetkellä tarkoitettua yksilöityä käyttötarkoitusta varten.

Mikäli kuluttaja **kieltää** IBA-mainonnan **yhdellä laitteella**, tämä kielto koskee myös muita laitteita, jotka ovat yhteydessä laitteeseen, jolla kielto tehtiin. Jos kaikista yrityksen IBA-mainontaan liittyvistä seurantatavoista ei voi kieltäytyä, tästä pitää ilmoittaa kuluttajalle selkeästi.

Kerättäessä **arkaluontoisia tietoja** IBA-segmenttejä varten, on verkkokäyttäjältä saatava erikseen **suostumus** tietojen käyttämisestä IBA-mainonnassa. IBA-mainontaa varten kerättyjä tietoja saa säilyttää vain niin kauan kuin se on tarpeen liiketoiminnassa. Tietojen turvaamiseksi yrityksen täytyy myös huolehtia fyysisistä, elektronisista ja hallinnollisista turvajärjestelyistä.

Internetin käyttäjälle tulee antaa mahdollisuus päättää, saako hänen tietojansa kerätä IBA-mainonnan kohdistamista varten.





Profilointi voi pohjautua muun muassa asiakkuudesta kerääntyneeseen tietoon, evästeiden avulla nettikäyttäytymisestä saatavaan tietoon tai henkilö on voinut itse suoraan kertoa mistä on kiinnostunut ja esimerkiksi ilmaissut haluavansa saada mielenkiinnonkohteestaan suoramarkkinointia.

Profilointia hyödynnetään internetin kohdennetuissa mainoksissa, joissa pyritään esimerkiksi evästeiden avulla tavoittamaan potentiaalisimmat asiakkaat.

Yleisen tietosuoja-asetuksen mukaan henkilöllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi, kuten profiloinnin, jolla on häneen kohdistuvia oikeusvaikutuksia tai joka muuten vaikuttaa häneen vastaavalla tavalla. Taloudelliset vaikutukset (esimerkiksi hintasyrjintä) voidaan katsoa oikeusvaikutuksia vastaaviksi vaikutuksiksi.

Markkinointiin liittyvällä profiloinnilla on harvemmin kovin dramaattisia vaikutuksia kohderyhmänsä elämään, kun se on tehty huolellisesti. Lisäksi markkinoijalla on oikeus itsenäisesti arvioida kenen se luulisi olevan kiinnostunut sen palveluista ja tarjota niitä heille itse määrittelemillään ehdoilla, kunhan se ei syyllisty syrjintään.

Profilointi on **lähtökohtaisesti sallittua** markkinoinnissa ilman henkilöltä erikseen saatua suostumusta. Henkilöllä on kuitenkin mahdollisuus vastustaa milloin tahansa hänen henkilötietojensa käsittelyä suoramarkkinointia varten, mikä kattaa siis profiloinnin hyödyntämisen markkinoinnissa.

Profilointia saa käyttää, jos se on välttämätöntä sopimuksen tekemistä tai täytäntöönpanoa varten, rekisteröidyn oikeuksien ja vapauksien suojaamiseksi tai rekisteröity on antanut profiloinnille nimenomaisen suostumuksensa.

Profiloinniksi ei katsota esim. tilannetta, jossa lainanantaja, tekee yleisen elämänkokemuksensa perusteella arvion, miten toinen henkilö tulee käyttäytymään. Jos lainantaja käyttää arviossaan hyödyksi tietokonetta ja algoritmeja, niin silloin kyse on profiloinnista.

3.4 Suoramarkkinointi ja asiakasviestintä

Perinteisellä suoramarkkinoinnilla tarkoitetaan puhelimitse tai postitse tapahtuvaa markkinointia. **Sähköisellä suoramarkkinoinnilla** tarkoitetaan markkinointia, joka tapahtuu sähköisesti esimerkiksi automatisoitujen soittojärjestelmien, faxien, sähköpostiviestien, tekstiviestien, puheviestien, ääniviestien tai kuvaviestien välityksellä.

Asiakasviestintänä pidetään viestintää, jonka tarkoituksena on asiakassuhteen hoitamiseksi tarvittava yhteydenpito, mihin ei liity markkinointia. Organisaatio saa itse valita mitä tapaa, kuten esimerkiksi sähköpostia ja tekstiviestiä, se käyttää asiakasviestinnässään. Asiakkaalla ei ole laillista oikeutta kieltäytyä häntä koskevasta asiakasviestinnästä.

Organisaatio saa lähettää asiakkailleen ja jäsenilleen asiakasviestintää **uutiskirjeinä**, kunhan ne eivät sisällä mainoksia. Suoramarkkinointia sisältävän uutiskirjeen lähettämiseen vaaditaan vastaanottajalta lupa.

Kuluttajalle saa tehdä markkinointia perinteisillä menetelmillä vapaasti ilman ennakkosuostumusta. Kuluttaja voi kuitenkin halutessaan kieltää markkinoinnin ja hänelle tulee kertoa kielto-oikeudesta asiakassuhteen tai muun yhteydenpidon aloitushetkellä esimerkiksi tietosuojaselosteen avulla.

Myyntipuhelun tai tapahtumakutsun hyväksyminen puhelimessa edellyttää kuluttajalta kirjallista jälkivahvistusta soiton jälkeen. Kirjallinen jälkivahvistus voi olla esimerkiksi tekstiviesti, johon vastaamalla kuluttaja hyväksyy tarjouksen tai osallistumisen tapahtumaan. Mikäli asiakas on itse yhteydessä yritykseen tai on jättänyt yhteydenottopyynnön yritykselle, ei jälkivahvistusta tarvita.

Markkinointipuheluja saa nauhoittaa puhelun sisällön todentamiseksi sekä koulutustarkoitusta tai laadun tarkkailua varten. Asiakkaalle tulee kertoa nauhoittamisesta mahdollisimman pian puhelun alettua.

Kuluttajalle ja potentiaaliselle asiakkaalle saa tehdä sähköisiä viestimiä hyödyntäen tarjouksia, vain silloin kun hän on antanut siihen **etukäteen suostumuksensa**.

Markkinointiviesteihin täytyy muistaa laittaa mukaan **tietosuojainformaatio** esimerkiksi linkin muodossa sekä kertoa viestin vastaanottajalle **kielto-oikeudesta**. Sähköposteihin voi laittaa esimerkiksi ”klikkaa tästä, jos et halua jatkossa vastaanottaa viestejämme” -linkin. Tekstiviesteissä kielto-oikeudesta voi kertoa esimerkiksi ”Kiellot: 0800 xxxx” tekstillä viestin lopussa. Puhelusta ei saa periä erillistä maksua.

Lupapyyntöjä varten kuluttajalle pitää antaa tarpeeksi informaatiota käsittelyn tarkoituksista ja tavoista sekä minkälaista suoramarkkinointia (viikkokirje, tarjous, kutsut jne.) hän tulisi saamaan, jotta hän voi arvioida mihin on suostumassa. Esimerkiksi EU:n tietosuojaviranomaisten mukaan sähköpostin ja tekstiviestin lähettämisestä tulisi kysyä lupa kahdella erillisellä kysymyksellä.

Lupapyyntöjä ei tarvita **poikkeuksellisesti** silloin kun palvelun tarjoaja tai tuotteen myyjä lähettää asiakkaalle sähköistä suoramarkkinointia omista samaan tuoteryhmään kuuluvista palveluista tai tuotteista esimerkiksi sähköpostitse tai tekstiviestinä. Palvelun tarjoajan tai tuotteen myyjän on kuitenkin täytynyt saada asiakkaan yhteystiedot palvelun tai tuotteen myynnin yhteydessä.

Yritysten yhteyshenkilöihin saa olla yhteydessä ilman etukäteen annettua suostumusta niin perinteisen kuin sähköisen suoramarkkinoinnin keinoin, kunhan yhteydenotot liittyvät jollain tavalla yrityksen toimintaan. Suoramarkkinointi tulee kuitenkin lopettaa, mikäli vastaanottaja kieltää sen.

Yrityksille ei saa lähettää kuluttajille suunnattua markkinointia, vaan suoramarkkinointiviestin sisällön pitää olla kohderyhmälle sopiva.

Mahdollisesta sähköisestä asiakasviestinnästä asiakkaalle, kuten lähetyksen tilanteen ilmoittamisesta tekstiviestillä, olisi suositeltavaa informoida kuluttajaa jo henkilötietoja kerättäessä, vaikka lainsäädännön puitteissa sitä ei vaadita. Selkeä informointi viestintäkäytännöistä kasvattaa asiakkaiden luottamusta organisaatiota kohtaan.

Tapahtuman markkinointi ja asiakasviestintä

Asiakastapahtuman markkinointia koskevat samat säännöt kuin suoramarkkinointia ja asiakasviestintää. **Kuluttajille** tapahtumakutsun lähettäminen kirjeitse tai siitä puhelimitse tiedottaminen on sallittua ilman ennakkosuostumusta. Sähköpostimarkkinointi edellyttää ennakkosuostumuksen.

Yrityksille tapahtumakutsun lähettäminen kirjeitse tai sähköpostitse on sallittua ilman ennakkosuostumusta. Myös puhelinmarkkinointi tapahtumasta on sallittua. Yrityksille kannattaa lähettää puhelimessa sovitusta tapahtumaan osallistumisesta esimerkiksi linkki sähköpostiin, jossa yritys voi käydä vahvistamassa osallistumisensa.

Sallittu suoramarkkinointi ja asiakasviestintä	B2C	B2B
Perinteinen suoramarkkinointi ilman ennakkosuostumusta	✓	✓
Sähköinen suoramarkkinointi ilman ennakkosuostumusta	✗	✓
Sähköinen suoramarkkinointi ennakkosuostumuksella	✓	✓
Mahdollinen asiakasviestintä sähköisesti ja perinteisesti	✓	✓

3.5 Valo- ja videokuvaus, webinaarit ja osallistujalistat

Valo- ja videokuva lasketaan yleisen tietosuoja-asetuksen mukaisesti henkilötiedoksi, jos siinä esiintyvä henkilö tai henkilöt ovat selvästi tunnistettavissa. Tällaisten valo- ja videokuvien käyttämiseen esimerkiksi markkinointitarkoituksiin tulee kysyä lupa kuvan kohteelta.

Lupaa voidaan kysyä esimerkiksi ilmoittautumisen yhteydessä, jolloin valokuvaajaa varten on hyvä erotella henkilöt ketkä suostuvat kuvattavaksi.

Vapaaehtoinen asettautuminen kuvattavaksi tapahtumaan rakennetun **kuvausseinän** eteen, käy suostumukseksi siihen, että kuva voidaan julkaista. Erillistä kirjallista suostumusta ei tarvita, mutta tällaistakaan kuvaa ei saa käyttää mainoksessa ilman henkilön suostumusta.

Mikäli tapahtumasta otetusta **yleiskuvasta** ei pysty tunnistamaan erityisesti ketään henkilöä, saa kuvan esimerkiksi jakaa sosiaalisessa mediassa, ilman etukäteen kysyttyä lupaa.

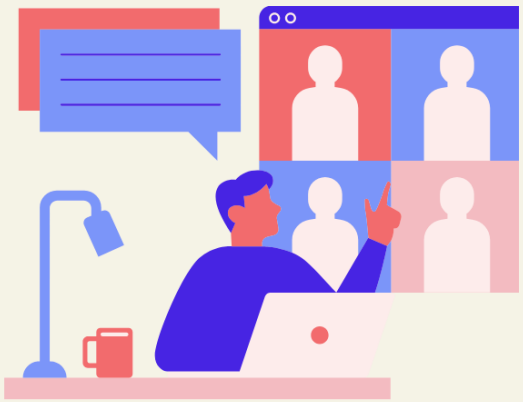
Webinaarin teknisenä alustana kannattaa käyttää yleisesti tunnetun yrityksen webinaarin pitämiseen tarkoitettuja sovelluksia, koska henkilötietoja jaetaan sovelluksen kautta niin sanotusti kolmannelle osapuolelle.

Dronella kuvaaminen on sallittua julkisilla paikoilla, kuten kaduilla, toreilla, metsissä tai muissa yleisölle julkisissa tiloissa. Erillinen lupa vaaditaan, jotta dronea voi lennättää taajamissa ja ihmisten yläpuolella. Toisen henkilön asunnon tai sen ikkunan edessä kuvaaminen on kiellettyä. Traficomin ylläpitämältä droneinfo-sivulta on mahdollista tarkistaa alueet, joilla dronen lennättäminen on kiellettyä.

Webinaaria tai muuta etätapahtumaa järjestettäessä on mietittävä etukäteen mitä yksityisyyteen liittyviä tietokoneen asetuksia hyödynnetään, tallennetaanko webinaari ja mitä tallenteelle tehdään.

Webinaaria varten kerätään usein siihen osallistuvien henkilöiden nimet, sähköpostiosoitteet ja joskus jopa sijaintitiedot. Näiden tietojen käsittelyä ja säilyttämistä varten tarvitaan jokin tietosuoja-asetuksen mukainen peruste, kuten webinaariin osallistuvan henkilön suostumus tai muu peruste.

Webinaariin osallistuvia henkilöitä on myös informoitava, mikäli heidän tietojaan näkyy webinaarin aikana muille osallistujille tai tilaisuudesta otetulla tallenteella.



Tapahtumanjärjestäjä voi käyttää suostumuksen lisäksi henkilötietojen jakamisen perusteena esimerkiksi oikeutettua etua osallistujalistojen laatimiseen ja nimikylttien käyttämiseen, mikäli tapahtuman luonne vaatii sen onnistuakseen.

Esimerkiksi **verkostoitumistapahtumien** kaltaisissa tapahtumissa osallistujat voivat hyvinkin odottaa, että heille jaetaan osallistujalistoja ja nimikylttejä verkostoitumista varten.

Ennen tapahtumaa on kuitenkin hyvä kertoa ilmoittautumisen yhteydessä, miten osallistujien tietojaan aiotaan käyttää ja antaa mahdollisuus kieltäytyä nimikylttien käytöstä, jos osallistuja ei halua tietojaan muiden näkyviin.

Jos tapahtumaan osallistuja itse antaa **käyntikorttinsa** esimerkiksi tapahtumanjärjestäjälle tai jonkin muun organisaation edustajalle, niin tämä tulkitaan suostumukseksi henkilötietojen, eli kortissa olevien tietojen käsittelyyn ja säilyttämiseen.

Kortin tietojen avulla saa olla sen antaneeseen henkilöön yhteydessä perinteisen tai sähköisen suoramarkkinoinnin keinoin riippuen onko kortin antanut henkilö tavallinen kuluttaja vai yrityksen edustaja.

Yrityksen edustajalle saa lähettää sähköpostitse suoramarkkinointia kortin tietoja käyttäen, mutta tavalliselta kuluttajalta sähköiseen suoramarkkinointiin täytyy pyytää erikseen lupa.

3.6 Arvonnat, kilpailut ja SOME

Sosiaalisen median palvelujen tietosuojaan liittyvissä säännöissä saattaa olla paljon eroja ja niiden tietosuojainformaatiot voivat olla hankalasti löydettävissä.

Yrityksen käyttäessä sosiaalista mediaa, sille muodostuu yhteisrekisterinpitäjyys sosiaalisen median palveluntarjoajan, kuten Facebookin kanssa. Yhteisrekisterinpitäjyys syntyy silloin kun yrityksen julkaisut keräävät tykkäyksiä ja yrityksen omalle somekanavalle kerääntyy seuraajia.

Julkaistaessa yrityksen omille somekanaville videoita ja kuvia juhlista tai tapahtumista on niissä esiintyviltä henkilöiltä kysyttävä lupa heidän näkymisestään somejulkaisuissa ennen julkaisujen tekemistä.

Kerättäessä henkilötietoja somen kautta, pitää miettiä millä perustein tietoja kerätään. Silloin kun asiakassuhdetta ei vielä ole, niin oikeutettua etua voi olla mahdollista käyttää perusteena tietojen keräämiseen.

Somen kautta kerätessä tietoja, pitää huolehtia kaikkien tietosuojaperiaatteiden toteutumisesta, kuten rekisteröidyn oikeuksista, tietojen minimoinnista ja tietosuojainformaation antamisesta rekisteröidyille.

Arvontojen ja kilpailujen yhteydessä rekisterinpitäjä saa kerätä vain sellaisia henkilötietoja, jotka ovat oikeasti tarpeellisia kilpailun tai arvonnan suorittamiseksi. Kerättäessä henkilötietoja, rekisteröityä tulee informoida muun muassa siitä mihin tarkoitukseen tietoja tullaan käyttämään ja kuinka kauan tietoja säilytetään.

Mikäli kerättyjä henkilötietoja aiotaan käyttää arvontaan liittyvien yhteydenottojen lisäksi sähköiseen suoramarkkinointiin, tähän täytyy kysyä erikseen lupa rekisteröidyltä. Jos suoramarkkinointi-suostumusta käytetään arvontaan osallistumisen ehtona, kuluttajalle on kerrottava mahdollisuudesta kieltäytyä suoramarkkinoinnista myöhemmin.

#kilpailut

Järjestettäessä hashtag-arpajaiset tai -kilpailut, vaarana on, että satunnainen sosiaalisen median käyttäjä voi tulla vahingossa osallistuneeksi kilpailuun, jonka kampanjaehdoissa lukee, että markkinoija saa rajoittamattomat oikeudet käyttää tietyllä hashtagilla julkaistuja kuvia ja aineistoja esimerkiksi somekanavissaan.

Siksi onkin suositeltavaa, että hashtag arvonnoissa ja kilpailuissa käytettäisiin sanayhdistelminä yrityksen nimeä ja sellaista sanaa, joka viestii kaupallisesta kampanjasta. Lisäksi olisi hyvä, että kilpailun tai arvonnan aikana kampanjasta ja sen ehdoista tuotettaisiin paljon sisältöä yrityksen omiin sosiaalisen median kanaviin.

Sosiaalisen median kampanjoissa tulee noudattaa kyseisen palveluntarjoajan omia sääntöjä ja sopimusehtoja, jottei kampanja ole esimerkiksi mainostamista koskevien lakien tai yleistä tietosuoja-asetusta koskevien sääntöjen vastainen.

3.7 Tietosuoja tapahtuman jälkeen

Kuluttajapuolella tapahtuman jälkeiseen henkilötietojen tallentamiseen sekä suoramarkkinointiin on pyydettävä suostumus esimerkiksi tapahtuman ilmoittautumisvaiheessa.

Palautteen pyytäminen sähköisesti ei ole markkinointia vaan asiakasviestintää, eikä siksi edellytä ennakkosuostumusta. Tosin siitä on silti hyvä informoida tietosuojaselosteessa yhtenä tiedon käyttötarkoituksista.

Jos tarkoituksena on kerätä potentiaalisia asiakkaita palautteen jättäneiden henkilötietojen avulla, **kuluttajilta** tulee palautteenannon yhteydessä kysyä lupa sähköiseen suoramarkkinointiin ja ilmoittaa mikäli tietoja aiotaan käyttää perinteiseen suoramarkkinointiin.

Jos osallistuja ei ole vielä valmiiksi asiakasrekisterissä, **B2B** puolella ei edellytetä henkilön suostumusta hänen liittämiseensä asiakasrekisteriin tai potentiaalirekisteriin.

Silloin kun kyseessä on olemassa oleva yritysasiakas, asiakkuuteen liittyen on usein mielekästä tallentaa tieto siitä, mihin tilaisuuksiin ja asiakastapahtumiin hän on osallistunut. Tällöin asiakkaalle voidaan kohdentaa esimerkiksi asiakastapahtumaan osallistumiseen liittyviä etuja ja alennuksia.

Tulostettujen ja sähköisten **osallistujalistojen** hävittämisestä tapahtuman jälkeen kannattaa sopia alihankkijoiden, kuten järjestysmiehiä tarjoavan palvelunjärjestäjän kanssa.

Tapahtuman jälkeen kaikki **tarpeettomiksi** muuttuneet **henkilötiedot** on hyvä poistaa viipymättä. Esimerkiksi osallistujien ruokavalinnat ja muut tapahtuman käytännönjärjestelyihin liittyvät henkilökohtaiset tiedot ja muut valinnat kannattaa poistaa heti kun niitä ei enää tarvita.

Webinaaritallenteesta kannattaa jälkikäteen anonymisoida, eli sumentaa tai rajata osallistujien nimet pois kuvasta, vaikka tallenne säilytettäisiin pelkästään sisäistä käyttöä varten.

Mikäli webinaaritallenteeseen jätetään siihen osallistuvien henkilöiden nimet näkyviin, tästä tulee informoida etukäteen kaikkia webinaariin osallistuvia ennen webinaarin tallennusta ja jakamista.

Jos tapahtumasta jaetaan sähköpostitse tallenteita tai muuta materiaalia osallistujille, sähköpostiviestin saajille ei saa tulla ilmi kelle kaikille muille sähköpostiviesti on myös lähetetty.

Jos tallenteen katselun yhteydessä tallentuu tieto siitä, kuka on katsellut tallennetta ja sen perusteella tehdään päätöksiä siitä, kehen otetaan yhteyttä myyntitarkoituksessa. Niin tästä tulee informoida etukäteen osallistujia ja tallenteen katselijoita.

Kutsuminen seuraavaan tapahtumaan

Oikeus lähettää kutsu seuraavaan tapahtumaan riippuu siitä, onko tapahtumaan osallistunut henkilö asiakas, kuluttaja vai yritysasiakas ja siitä miten seuraavan tapahtuman kutsu hänelle lähetetään.

Jos tapahtumaan osallistunut henkilö on antanut suostumuksensa yhteystietojensa käyttöön tulevia tapahtuman markkinointitarkoituksia varten, voi hänelle edelleen lähettää markkinointimateriaalia tulevasta tapahtumasta

Jos henkilöä on informoitu, että hän saa vuosittain kutsun vastaavanlaiseen tapahtumaan, eikä hän ole kieltänyt kutsun lähettämistä. Niin hänelle voi lähettää kutsun uuteen tapahtumaan. Esimerkiksi asiakkaille ja jäsenille voi yleensä huolettaa lähettää kutsuja tapahtumiin, jos he eivät erikseen ole kertoneet, etteivät halua kutsuja.

Terveystietoja tai muita arkaluontoisia tietoja sisältävissä kirjeissä sisällön ei pitäisi näkyä kirjekuoren ikkunasta ulkopuolelle. Ainoastaan kirjeen vastaanottajan nimi ja osoite saavat näkyä kirjeestä.

04
Muistilistoja & esimerkkejä

4.1 Tietosuojallisen asiakastilaisuuden muistilista

Kuvitellaan, että terveysteknologia alalla toimiva suomalainen yritys X Oy on järjestämässä **asiakastilaisuuden** pääkonttorillaan, jonne se on kutsumassa alan yrityksiä testaamaan X Oy:n uusia myyntiin tulevia röntgenlaitteita. Tapahtuma kestää kaksi päivää ja tilaisuudessa vieraille tarjoillaan hienoja ruokia ja juomia, sekä tapahtumasta tehdään X Oy:n someen julkaisuja. Tilaisuudesta kerätään myös palautetta.

- Osallistujia tulee informoida mihin tarkoitukseen heidän henkilötietoja käytetään ja kuinka kauan tietoja tullaan säilyttämään.
- Tapahtumalle kannattaa mahdollisesti tehdä oma tietosuojaseloste.
- Tapahtuman henkilötietojen käsittelyä suunniteltaessa kannattaa olla tarvittaessa yhteydessä yrityksen tietosuoja-asiantuntijoihin, kuten tietosuojavastaavaan.

Ennen tapahtumaa

- Yrityksille saa lähettää markkinointimateriaalia tapahtumasta sähköpostitse, soittamalla tai tekstiviestitse
- Henkilöille, jotka ovat ostaneet samankaltaisia tuotteita X Oy:ltä, saa lähettää tapahtumasta markkinointimateriaalia sähköpostitse ja tekstiviestein, jos he eivät ole sitä erikseen kieltäneet.
- Tietojenkäsittelysopimukset täytyy tehdä ulkopuolisten yritysten (kuten valokuvaajan ja catering-palvelun) kanssa, jotka tulevat käsittelemään osallistujien henkilötietoja.
- Markkinointiviestien mukaan tulee laittaa tietosuojainformaatio ja kertoa kielto-oikeudesta
- Osallistujia on Informoitava ja mahdollisesti kysyttävä suostumusta, mikäli heidän henkilötietoja tulee näkymään esimerkiksi webinaareissa tai nimilapuissa muille osallistujille.
- Jos tapahtumaa mainostetaan X Oy:n nettisivuilla sijaintitietoja hyödyntäen, täytyy tietojen hyödyntämiseen kysyä lupa nettisivulle tultaessa.
- Tietojen minimoinnin periaate, eli kerää osallistujilta vain oikeasti tarpeellista tietoa
- Kysy suostumusta arkaluontoisten tietojen (esim. tiedot allergioista) säilyttämiseen.

Tapahtuman aikana

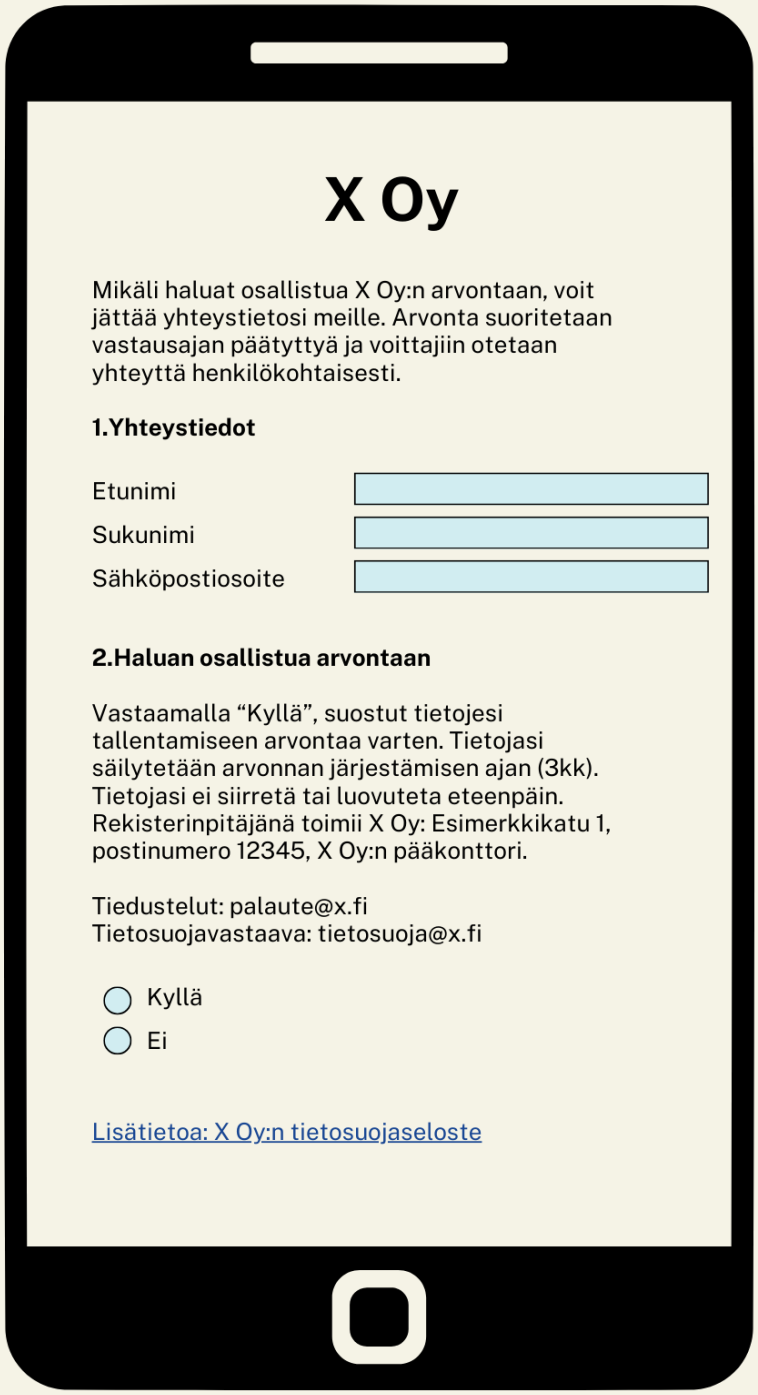
- Vieraita, jotka ovat antaneet luvan kuvaamiselle ilmoittautumisen yhteydessä, saa kuvata.
- Vapaaehtoinen asettautuminen kuvattavaksi tapahtumaan rakennetun kuvausseinän eteen, käy suostumukseksi siihen, että kuva voidaan julkaista somessa.
- Mikäli tapahtumasta otetusta yleiskuvasta ei pysty tunnistamaan erityisesti ketään henkilöä, saa kuvan esimerkiksi jakaa sosiaalisessa mediassa, ilman etukäteen kysyttyä lupaa.
- Arvontojen ja kilpailujen yhteydessä saa kerätä vain oikeasti tarpeellisia tietoja kilpailun tai arvonnan suorittamiseksi. Jos kerättyjä henkilötietoja aiotaan käyttää sähköiseen suoramarkkinointiin, tähän täytyy kysyä erikseen lupa rekisteröidyltä.
- Hashtag arvonnoissa ja kilpailuissa olisi hyvä käyttää sanayhdistelmiä, jotka viestivät kaupallisesta kampanjasta.

Tapahtuman jälkeen

- Palautteen pyytäminen sähköisesti on sallittua, mutta siitä on silti hyvä informoida tietosuojaselosteessa yhtenä tiedon käyttötarkoituksista.
- Jos osallistuja ei ole vielä valmiiksi asiakasrekisterissä, B2B puolella ei edellytetä henkilön suostumusta hänen liittämiseensä asiakasrekisteriin tai potentiaalirekisteriin.
- Tapahtuman jälkeen kaikki tarpeettomiksi muuttuneet henkilötiedot on poistettava viipymättä.
- Webinaaritallenteesta tulee jälkikäteen anonymisoida, eli sumentaa tai rajata osallistujien nimet pois kuvasta, vaikka tallenne säilytettäisiin pelkästään sisäistä käyttöä varten.
- Jos vieras ei ole kieltäytynyt, voi hänelle lähettää markkinointimateriaalia tulevasta ensi vuoden tapahtumasta.

4.2 Esimerkki arvontalomakkeesta

Kuvitellaan, että X Oy lähettää asiakastilaisuuden jälkeen siihen osallistuneille henkilöille palautekyselyn. Jos palautekyselyn yhteydessä on mahdollisuus osallistua arvontaan, niin arvontalomake voi näyttää esimerkiksi tältä.



05

Usein Kysytyt Kysymykset

5.1 Mistä saa apua?

Tietosuojaan liittyvät asiat voivat tuntua monimutkaisilta ja vaikeasti käsiteltäviltä. Onneksi apua tietosuoja-asioihin on hyvin saatavilla.

Eräs hyvä verkkosivusto, josta saa apua tietosuojaan liittyviin kysymyksiin on tietosuojavaltuutetun toimiston nettisivut (**www.tietosuoja.fi**). Lisäksi yrityksen tietosuoja-asiantuntijoiden ja tietosuojavastaavan puoleen voi aina kääntyä kun tietosuoja-asiat mietityttävät.

5.2 Usein kysyttyjä kysymyksiä

Mistä tiedän tarvitsenko tapahtumaani varten erillistä tietosuojaselostetta?
Tämä riippuu täysin tapahtuman luonteesta, ja siitä mitä henkilötietoja kerätään. Tämän asian kanssa kannattaa olla yhteydessä yrityksen tietosuojavastaavaan.

Mistä tiedän kuinka kauan tapahtumasta otettuja henkilöiden kuvia saa säilyttää?
Yleisessä tietosuoja-asetuksessa ei ole tähän selkeää vastausta. Tietosuojaperiaatteiden mukaan kuvia saa säilyttää niin kauan kuin ne ovat tarpeellisia. Siksi tapahtuman tietosuojaselosteessa kannattaa mainita, kuinka kauan tapahtumasta otettuja kuvia tullaan säilyttämään, jonka jälkeen ne poistetaan.

Pitäisikö minun, yrityksen markkinointitiimin jäsenen, osata tehdä tietosuojaseloste tai tietojenkäsittelysopimus?
Ei pidä osata. Sopimuksista ja selosteista voi olla yhteydessä esimerkiksi yrityksen tietosuojavastaavaan.

Mistä tiedän, mitä viestimiä pitkin markkinointiviestejä saa laittaa asiakkaille?
Tietosuojaperiaatteiden mukaan asiakkaista kerättyjä tietoja saa käyttää vain tiettyä ennalta määriteltyä tarkoitusta varten, eikä rekisterinpitäjä saa käyttää tietoja myöhemmin muulla tavoin. Eli vastaus riippuu käytännössä siitä, mihin tarkoitukseen henkilötiedot on kerätty ja kuinka asiakasta on informoitu tietojen käytöstä suoramarkkinointiin liittyen.

Esimerkiksi jos asiakkaalle ei ole informoitu tietojen keräämisen yhteydessä, että häneen saatetaan olla yhteydessä toisesta saman konsernin yrityksestä, niin markkinointiviesti toiselta yritykseltä voi aiheuttaa hämmennystä asiakkaassa. Tämän vuoksi asiakkaan informoimiseen ja sähköisen suoramarkkinoinnin lupapyyntöihin tulee kiinnittää erityistä huomiota tietojen keräämisen yhteydessä.

Haluan käyttää ulkopuolisen yrityksen tarjoamaa nimilistaa suoramarkkinointiin, mitä teen?
Kyseisessä tilanteessa on tarkistettava, onko yrityksellä oikeus luovuttaa lista ja onko listalla olevien henkilöiden tiedot kerätty laillisesti. Laillisuuden voi tarkistaa esimerkiksi pyytämällä yritykseltä nähtäväksi suostumuslomakkeet, joissa näkyy henkilöiden suostumus tietojen keräämiseen ja luovuttamiseen eteenpäin.