Haaga-Helia
ammattikorkeakoulu Oy

EU:n tietosuoja-asetuksen 2016/679 mukaisen tietotilinpäätöksen laatiminen ulkoistettua asiakashankintaa harjoittavassa yrityksessä

Juha Leskinen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Juha Leskinen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön nimi
EU:n tietosuoja-asetuksen 2016/679 mukaisen tietotilinpäätöksen laatiminen ulkoistettua asiakashankintaa harjoittavassa yrityksessä

Sivu- ja liitesivumäärä
22 + 12

Tämän opinnäytetyön toimeksiantajana oli ulkoistettua asiakashankintaa harjoittava yritys, jolle laadin EU:n tietosuoja-asetuksen mukaisen tietotilinpäätöksen.

Opinnäytetyön johdannossa teen lyhyen katsauksen tietosuoja-asetukseen ja sen vaikutuksesta rekisterinpitäjiin ja kerron rajaavani pois nykyisiin lakeihin perustuvat seikat.

Tieto-osuudessa käyn asetusta läpi toimeksiantajan näkökulmasta, mitä vaatimuksia rekisterinpitäjille ja -käsittelijöille on säädöksessä määrätty sekä mitä oikeuksia rekisteröidyille luonnollisille henkilöille säädöksessä annetaan. Lisäksi sivuan säädöksen tuomia muutoksia nykyiseen lainsäädäntöön.

Asetuksen vaatimusten ja oikeuksien perusteella katson, miten Yritys on miellettävä rekisterien käsittelyn kannalta ja käyn läpi mitä haasteita työssäni koin. Käyn läpi toimeksiantoni aikana tapahtuneet keskeiset muutokset Yrityksen toiminnassa ja muutosten vaikutuksia työni tekemiseen. Tuon esiin perustellusti, mitkä olivat keskeiset uudistuksen Yritykselle toimeksiantoni johdosta.

Vertaan tietotilinpäätöksen ja tietosuoja-asetuksen asiasisältöjä keskenään sekä pohdin mitä tämän työn tekeminen on minulle opettanut ja mitä muuttaisin toiminnastani, jos tekisin tietotilinpäätöksen uudelleen.

Asiasanat
Tietotilinpäätös, Tietosuoja-asetus, Tietosuoja, GDPR

Sisällys

1 Johdanto 1
1.1 Tavoitteet ja rajaukset 1
1.2 Lyhenteet ja käsitteet 2
2 EU tietosuoja-asetuksen läpikäyntiä 4
2.1 Henkilötiedon määritelmä 4
2.2 Rekisteröidyn oikeudet 5
2.2.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä 5
2.2.2 Oikeus saada pääsy tietoihin 5
2.2.3 Tietojen oikaisu ja unohtaminen 6
2.2.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän ilmoitus velvollisuus 6
2.2.5 Oikeus siirtää tiedot järjestelmästä toiseen 7
2.2.6 Vastustamisoikeus 7
2.2.7 Automatisoidut yksittäispäätökset ja profilointi 7
2.3 Rekisterinpitäjän velvollisuudet 7
2.3.1 Sisäänrakennettu ja oletusarvoinen tietosuoja 8
2.3.2 Oikeusperusta 8
2.3.3 Osoitusvelvollisuus 9
2.4 Riskiperusteinen lähestymistapa 9
2.5 Tiedonanto, yhteistyövelvoite ja tietoturvaloukkaukset 10
2.6 Tietoturva 10
2.7 Keskeiset uudistukset aiempaan lainsäädäntöön verrattuna 10
3 Yrityksen esittely 11
3.1 Suunnitelma 11
4 Dokumentin luominen Yritykselle 12
4.1 Toteutus 12
4.1.1 Haasteet toteutuksessa 13
4.2 Tuotos 14
4.2.1 Rekisteritietojen liikkuminen 14
4.2.2 Tietosuojavuosikello 17
4.2.3 Ristiintaulukointi 18
4.3 Mikä muuttui 19
5 Pohdinta ja johtopäätelmät 20
5.1 Oman oppimisen arviointi 21
Lähteet 23
Liitteet 25
Liite 1. Tietotilinpäätös 25

1 Johdanto

Tietosuoja- ja tietoturva-asioiden käsittely valtakunnallisissa uutisissa on lisääntynyt tänä keväänä valtavasti. Syitä tähän ovat lisääntyneet identiteettien varkaudet, yrityksiin kohdistuneet tietomurrot ja henkilöistä kerättyjen tietojen väärinkäytökset. Näistä uutisista suurimpina voi mainita Facebookin tietojen päätymisen Gambridge Analytica yritykselle, joka käytti tietoja vastoin sopimuksia. Tässä tapauksessa jopa 50 miljoonan Facebookin käyttäjän tiedot kerättiin ja niitä käytettiin esimerkiksi kohdennettuihin vaalimainoksiin Yhdysvaltojen presidentin vaaleissa. (Laine 2018.)

Lisäksi suurta ”pöhinää” tietosuojan ympärillä aiheuttaa Euroopan Unionin tietosuoja-asetus 2016/679. Tämän kansallisia tietosuojalainsäädäntöjä yhtenäistävän asetuksen EU hyväksyi 27.4.2016. Asetus astui tuolloin voimaan, mutta sen käyttöönottoon annettiin siirtymäaika, joka päättyy 25.5.2018. Asetus koskee kaikkia yrityksiä ja yhteisöitä, jotka käsittelevät henkilötietoja.

Tästä asetuksesta johtuen kaikkien rekisterienpitäjien ja rekisterinkäsittelijöiden tulee toimia asetuksen mukaisesti viimeistään 25.5.2018 alkaen. Tämän vuoksi yritysten ja yhteisöjen pitää pystyä osoittamaan toimivansa asetuksen mukaisesti. Eräs tapa osoittaa toimivansa vaatimusten mukaisesti on tehdä tietotilinpäätös. Tähän vaihtoehtoon päätyi Yritys, jonka toimeksiantona tein sille tietotilinpäätöksen.

Toimeksiantajanani on suomalainen suuri ulkoistettua asiakashankintaa harjoittava yritys. Yritys toimii Toimeksiantajien ja asiakkaiden välissä sopien toimeksiantajille asiakastapaamisia. Yrityksen on tärkeää osoittaa sekä toimeksiantajille, että asiakkaille noudattavansa riittävää huolellisuutta ja toimivansa kaikissa asioissa tietoturvallisesti.

Toimeksiannon mukaisesti työn tavoitteena oli tehdä Yritykselle tietotilinpäätös ja samalla läpikäydä Yrityksen toimintatavat keskittyen erityisesti henkilörekistereiden käsittelyyn ja ehdottaa Yritykselle tietosuoja-asetuksen mahdollisesti vaatimia muutoksia nykyisiin toimintatapoihin.

1.1 Tavoitteet ja rajaukset

Tässä työssä on tarkoitus käsitellä tietosuoja-asetuksen tuomia velvollisuuksia ja oikeuksia sekä miten tietotilinpäätös Yritykseen tehtiin. Lisäksi käsittelen tietosuoja-asetuksen tuomat keskeiset uudet seikat yleisellä tasolla ja mitä mahdollisia vaikutuksia säädöksellä on Yrityksen toimintaan, dokumentaatioon ja kanssakäymiseen toimeksiantajien kanssa.

Työssä on rajattu pois laeissa erikseen määritellyt velvoitteet rekisterinpitäjille, koska ne eivät koske Yritystä.

1.2 Lyhenteet ja käsitteet

Artikla	Yksittäinen pykälä EU:n asetuksessa.
Asetus	EU:n lainsäädäntäväline, joka astuu sellaisenaan voimaan ja joka tarvittaessa kumoaa jäsenmaissa olevat päällekkäiset lait.
Bookkaus	Kohde, jolle sovittu tapaaminen.
Direktiivi	EU:n antama lainsäädäntäohje, joka antaa toimintaohjeita lakien säätämiseksi.
EU	Euroopan Unioni.
GDPR	General Data Protection Regulation. EU:n yleinen tietosuoja-asetus 2016/679.
Henkilötieto	Tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvää tietoa.
Kampanja	Liitteessä tarkoitettu projektiin liittyvä kohderyhmä / soittokausi.
Kohderyhmä	Liitteessä tarkoitetut henkilöt, joille puhelin markkinointia kohdistetaan.
Kolmas osapuoli	Taho, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.
Kontakti	Buukatut ja kieltäytyneet asiakkaat.
Käsittelijä	GDPR:ssä määritelty henkilötietojen käsittelyä rekisterinpitäjän toimesta tekevä taho.
NDA	Salassapitosopimus (non-disclosure agreement).

OM 4/2017 Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017.

Profilointi Henkilötietojen sellainen automaattinen käsittely, että tuloksista voidaan analysoida tai päätellä seikkoja jotka liittyvät henkilökohtaisiin ominaisuuksiin kuten kiinnostusten kohteet, terveys, työ tai matkustaminen.

Projekti Liitteessä tarkoitettu asiakassuhde / asiakkuus.

Rekisteri Mitä tahansa jäsenneltyä henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Rekisterinpitäjä
Henkilötietorekisterin käytöstä vastaava taho tai taho, jonka käyttöön se on perustettu.

Rekisteröity Luonnollinen henkilö, jonka henkilötietoja käsitellään.

Resitaali Artikloiden perustelut.

Tietosuoja-asetus 679/2016
Euroopan Parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus).

Tietotilinpäätös
Tapa, jolla yritys voi sisäisesti dokumentoida henkilötietojen käsittelyä ja siten täyttää tietosuoja-asetuksen osoitusvelvollisuutta.

Toimittaja Liitteessä tarkoitettu Yritykselle henkilötietoja eli kohderyhmiä Kampanjaan toimittava taho.

VRK Väestörekisterikeskus.

Yritys Liitteessä tarkoitettu toimeksiannon tehnyt yritys.

2 EU tietosuoja-asetuksen läpikäyntiä

Oikeusministeriössä oli käynnissä hanke ”Henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistaminen (TATTI – työryhmä)” (EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017:35), jonka tavoitteena oli arvioida nykyisen henkilötietolain (523/1999) toimivuus, sekä onko se ristiriidassa tietosuoja-asetuksen kanssa. Mahdollista uutta lakia säädettäessä voidaan käyttää hyväksi asetuksen jättämää kansallista liikkumavaraa.

> ”Työryhmän toimikausi on 17.2.2016 - 16.2.2018. Työryhmän tulee laatia ehdotuksensa lainsäädännön muutoksiksi hallituksen esityksen muotoon. Työryhmän tulee saada mietintönsä lainsäädännön muutosehdotuksista valmiiksi 31.5.2017 mennessä.” (EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017:35)

Työryhmä jätti mietintönsä kesäkuussa 2017, ja siinä se kertoi jatkavansa työtään 16.2.2018 asti. (EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017:35)

Hallitus on antanut eduskunnalle esityksen EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018), jonka tavoitteena on täydentää tietosuoja-asetusta, kuten valvontaviranomaisia koskevat säännökset ja käyttää asetuksen antama kansallinen liikkumavara nykyisen oikeustilan säilyttämiseksi mahdollisuuksien mukaan muuttumattomana. Lisäksi siinä esitetään kumottavaksi nykyinen henkilötietolaki sekä tietosuojalautakunnasta ja tietosuojavaltuutetusta annettu laki. Tarkoituksena on, että tämä tietosuoja-asetusta täydentävä laki ja tietosuoja-asetus muodostaisivat yhtenäisen kokonaisuuden (Finlex 2018).

Tietosuoja-asetus on kansallisesti suoraan sovellettava säädös siirtymäajan päättyessä 25.5.2018, jota kansallinen lainsäädäntö täydentää.

2.1 Henkilötiedon määritelmä

Tietosuoja-asetus koskee ainoastaan luonnollisia henkilöitä ja se määrittelee artiklassa 4 henkilötiedot seuraavasti:

> Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. (Tietosuoja-asetus 679/2016, artikla 4.)

Merkittävää tässä on toimeksiantoni kannalta se, että jos tiedot ylikirjoitetaan, ne voidaan edelleen säilyttää rekisterissä esimerkiksi sulkulistaa, raportointia ja tilastointia varten. Historiatiedon Yritys anonymisoi tilastointia varten.

2.2 Rekisteröidyn oikeudet

Tietosuoja-asetuksessa korostetaan rekisterinpitäjän velvollisuuksia. Siinä on myös korostettu rekisteröidyn oikeuksia huomattavasti enemmän kuin aiemmassa direktiivissä. Se jättää vastuun rekisteröidyn luonnollisen henkilön tietojen oikeellisuudesta rekisterinpitäjälle. Rekisterinpitäjän on myös huolehdittava rekisteröidyn oikeuksien toteutumisesta henkilötietojen käsittelyyn liittyvissä prosesseissa ja tietojärjestelmissä. (OM 4/2017, 23.)

2.2.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

Asetuksessa korostetaan avoimuutta ja annetaan henkilötietolakia tarkempia määräyksiä rekisterinpitäjän velvollisuuksista ja rekisteröidyn oikeuksista. Henkilön pyytäessä henkilötiedot on toimitettava tiiviisti, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa ilman aiheetonta viivytystä. Tietopyynnön johdosta aloitettuihin toimenpiteisiin pitää toimittaa pyytäjälle viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Kyseiseen määräaikaan on olemassa joitain poikkeuksia ja sitä voidaan tietyin ehdoin jatkaa. (Tietosuoja-asetus 679/2016, artikla 12.)

Tämä sama määräaika pätee myös ilmoitukselle rekisteröidylle, mikäli rekisterinpitäjä ei aio tietoja toimittaa. Jos rekisterinpitäjä kieltäytyy toimittamasta tietoja, on sen kerrottava mitä oikaisukeinoja rekisteröidyllä on, kuten tehdä valitus valvontaviranomaiselle. Sekä toimitetut tiedot, että toimenpiteet rekisteröidyn oikeuksien toteuttamiseksi ovat lähtökohtaisesti maksuttomia. Edellä mainittu kuukauden määräaika ei kuitenkaan päde, jos rekisteröity on jo saanut tiedot, tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa. (Tietosuoja-asetus 679/2016, artikla 14.)

2.2.2 Oikeus saada pääsy tietoihin

Rekisteröidyllä henkilöllä on oikeus saada pääsy omiin tietoihinsa ja saada jäljennös häntä koskevista henkilötiedoista. Tälle tietojen pyynnölle ei säädetty määrämuotoa. Jos tietopyyntö on tehty sähköisesti, niin tiedot pitää myös toimittaa yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää. (Tietosuoja-asetus 679/2016, artikla 12, artikla 15.), mutta jos rekisterinpitäjällä on syytä epäillä pyytäjän henkilöllisyyttä, niin rekisterinpitäjä voi pyytää lisätietoja pyytäjän henkilöllisyyden selvittämiseksi. Tämä sama

pätee myös rekisteröidyn pyytäessä muutoksia omiin tietoihinsa tai saada ne siirretyksi toiseen järjestelmään. (Tietosuoja-asetus 679/2016, artikla 12.)

2.2.3 Tietojen oikaisu ja unohtaminen

Tietosuoja-asetus antaa rekisteröidylle henkilölle oikeuden oikaista häntä koskevat virheelliset, epätarkat tai puutteelliset tiedot. Hänellä on myös oikeus toimittaa puuttuvia tietoja rekisterinpitäjälle.

Samoin rekisteröidyllä henkilöllö on oikeus pyytää poistamaan (oikeus tulla unohdetuksi) häntä koskevat tiedot, kun niitä ei enää käytetä siihen tarkoitukseen mihin ne on kerätty. Erityistä huomiota asetuksessa annetaan lapsena annetulle tiedoille. Nämä lapsena annetut tiedot voi myöhemmin aikuisena pyytää poistettavaksi (oikeus tulla unohdetuksi lapsena). (Tietosuoja-asetus 679/2016, artikla 17 ja resitaali 65.)

2.2.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän ilmoitus velvollisuus

Rekisteröidyllä on oikeus rajoittaa tietojensa käsittelemistä. Asetuksessa on mainittu erikseen neljä eri tilannetta tästä.

Jos tietojen oikeellisuus on epäselvää, käsittelyä voidaan rajoittaa siksi ajaksi, kun tietojen oikeellisuus selvitetään rekisterinpitäjän toimesta. (Tietosuoja-asetus 679/2016, artikla 18.)

Rekisteröidyn tietojen käsittely on lainvastaista ja rekisteröity ei halua niiden poistamista ja vaatii niiden käytön rajoittamista. Tiedot on hyvä säilyttää, jos tulee tarve selvittää väärinkäytös myöhemmin. (Tietosuoja-asetus 679/2016, artikla 18.)

Rekisterinpitäjä katsoo tiedot tarpeettomiksi, mutta rekisteröity tarvitsee niitä itse esimerkiksi oikeudellisiin tarkoituksiin. (Tietosuoja-asetus 679/2016, artikla 18.)

Julkista valtaa on voitu käyttää rekisteröintiin yleiseen etuun vedoten ja rekisteröity ei halua tietojaan käteltävän. Tällöin rekisteröity voi myös vaatia tietojen käsittelyn rajoittamista, kunnes asia selviää. (Tietosuoja-asetus 679/2016, artikla 18.)

Edellä mainittujen tapausten jälkeen tapahtuvasta tietojen käsittelyn jatkamisesta tulee asiasta ilmoittaa rekisteröidyille ja mahdollisille kolmansille osapuolille. (Tietosuoja-asetus 679/2016, artikla 19.)

2.2.5 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröity voi pyytää ja siirtää, toiseen rekisteriin sellaiset tiedot, jotka hän on toimittanut rekisterinpitäjälle, jos käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti. Tiedot pitää saada jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa nykyisen rekisterinpitäjän estämättä. Tiedot pitää siirtää suoraan rekisterinpitäjältä toiselle, mikäli se on teknisesti mahdollista. (Tietosuoja-asetus 679/2016, artikla 20.)

2.2.6 Vastustamisoikeus

Rekisteröidyllä on oikeus vastustaa hänen henkilötietojensa käyttämistä suoramarkkinointia varten. Tämä on Tietosuoja-asetuksen johdanto-osassa sanottu seuraavasti:

> ”Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä olisi oltava oikeus milloin tahansa ja maksutta vastustaa käsittelyä, mukaan lukien profilointia niiltä osin kuin se liittyy suoramarkkinointiin, olipa kyse sitten alkuperäisestä tai myöhemmästä käsittelystä. Tämä oikeus olisi nimenomaisesti saatettava rekisteröidyn tietoon ja esitettävä selkeästi ja muusta tiedotuksesta erillään.” (Tietosuoja-asetus 679/2016, johdanto-osan kohta 70.)

Tämä oikeus olisi lisäksi ilmoitettava viimeistään silloin, kun häneen ollaan yhteydessä ensimmäistä kertaa.

Lisäksi rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseen liittyvällä perusteella. Tällöin rekisterinpitäjä ei saa käsitellä rekisteritietoja, paitsi osoittamalla käsittelyyn olevan huomattavan tärkeä ja perusteltu syy. Lain perusteella pidettäviä julkisia rekistereitä tämä ei koske. (Tietosuoja-asetus 679/2016, artikla 21.)

2.2.7 Automatisoidut yksittäispäätökset ja profilointi

Asetus kieltää oikeusvaikutuksellisten automatisoitujen päätösten tekemisen esimerkiksi profilointiin perustuen, ellei rekisteröity ole antanut siihen erikseen lupaa. Profilointia ei ole sellaisenaan kielletty. (Tietosuoja-asetus 679/2016, artikla 4, artikla 22.)

2.3 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjälle on määritelty periaatteita henkilötietojen käsittelystä, joiden mukaan niitä on käsiteltävä rekisteröidyn oikeuksia ja vapauksia kunnioittavasti. Näitä periaatteita ovat:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

Näitä periaatteita on noudattava kaikissa tietojen käsittelyvaiheissa. Tämän vuoksi rekisterinpitäjän tulee myös pystyä osoittamaan noudattaneensa näitä periaatteita. Siksi rekisterin pitäjältä vaaditaan aiempaa tarkempaa suunnittelua ja dokumentointia. (Tietosuoja-asetus 679/2016, resitaali 39, artikla 5, artikla 6.)

2.3.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Oletusarvoista ja sisäänrakennettua tietosuojaa käsitellään asetuksen 25 artiklassa. Siinä sanotaan, että rekisterinpitäjän pitää itse arvioida henkilötietojen käsittelytapoja huomioiden uusimmat tekniikat ja niiden kustannukset, käsittelyn luonne ja laajuus. Lisäksi rekisterinpitäjän on kerättävä vain tarpeelliset tiedot juuri kyseistä tarkoitusta varten. Tämä käsittää henkilötietojen määrää, laajuutta, saatavilla oloa ja säilytysaikaa.

Edellä mainittujen seikkojen arvioinnin perusteella rekisterinpitäjän tulee järjestää henkilötietojen käsittely järkevästi. Käsittelytapoja määritettäessä otetaan huomioon käytettävissä olevat keinot ja käsittelyn laajuus ja luonne sekä tietojen kohteen oikeuksille aiheutuva riski. (Tietosuoja-asetus 679/2016, artikla 25.)

Määritellessään henkilötietojen käsittelytapoja rekisterinpitäjän on huolehdittava käsittelyn yhteydessä tietosuojantoteutumisesta teknisillä ja organisatorisilla toimenpiteillä. Näillä tarkoitetaan esimerkiksi henkilöstön kouluttamista ja ohjeistamista, salassapitosopimuksia, omavalvontaa, tietojärjestelmien tietoturvaa ja toiminnan auditointeja. (Tietosuoja-asetus 679/2016, resitaali 78.)

2.3.2 Oikeusperusta

Rekisterin pitäminen on 6 artiklan mukaan lainmukaista ainoastaan ja vain, jos jokin seuraavista edellytyksistä täyttyy:

- rekisteröity on antanut suostumuksen
- rekisteröity on osapuolena sopimuksessa, jota varten tiedot tarvitaan
- rekisterinpitäjällä on lakisääteinen velvoite

- rekisteröidyn tai toisen henkilön elintärkeä etu sitä vaatii
- käsittely julkisen vallan toimesta
- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut sitä vaativat

Asetuksessa huomioidaan erityisten henkilötietojen ryhmät, joiden käsittely on lähtökohtaisesti kielletty, ja sallittu ainoastaan tietyin perustein. Artiklassa 9 sanotaan:

> Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä. (Tietosuoja-asetus 679/2016 artikla 9.)

Lisäksi rekisterinpitäjän tulee arvioida syrjäyttääkö rekisteröidyn edut tai perusoikeudet ja -vapaudet rekisterinpitäjän oikeudet rekisterin pitämiselle, varsinkin jos kyseessä on lapsi. Lapsen ikärajan määrittäminen liittyy tietoyhteiskunnan palveluiden tarjoamiseen ja niihin suostumuksen antamiseen. Asetuksessa lapseksi määritellään alle 16-vuotiaat, mutta asetus antaa kansalliselle lainsäädännölle liikkumavaraa lapsen iän kanssa kuitenkin siten, että iän pitää olla vähintään 13 vuotta. (Tietosuoja-asetus 679/2016, artikla 8, resitaali 38.)

2.3.3 Osoitusvelvollisuus

Rekisterinpitäjällä on oltava kyky osoittaa noudattavansa asetuksen määräyksiä käsitellessään henkilötietoja, myös käytännössä. (Tietosuoja-asetus 679/2016, artikla 5) Tämä käytännössä tarkoittaa henkilötietojen käsittelyn prosessien ja tietoturvan käytännön toteuttamisen dokumentointia. Yhtenä keinona esitetään myös tietosuoja-asetuksen mukaisia sertifikaatteja ja käytännesääntöjä, joilla voidaan osoittaa velvollisuuksia noudatettavan. (OM 4/2017, 14.)

2.4 Riskiperusteinen lähestymistapa

Rekisterinpitäjän on suhteutettava tietosuoja-asetuksen asettamat velvollisuudet ja henkilötietojen suojaustoimet näihin kohdistuviin riskeihin ja tehtävä arvio näistä riskeistä. Arviossa on huomioitava henkilötietojen käsittelyn luonne, laajuus ja asiayhteys. Rekisterinpitäjän on toteutettava päivitettävissä olevat tekniset ja organisatoriset toimenpiteet, joilla voidaan osoittaa tämän asetuksen noudattaminen. (Tietosuoja-asetus 679/2016, artikla 24.)

2.5 Tiedonanto, yhteistyövelvoite ja tietoturvaloukkaukset

Rekisterinpitäjän on ilman aiheetonta viivytystä, mahdollisuuksien mukaan 72 tunnissa, ilmoitettava tietoturvaloukkauksista valvontaviranomaiselle, paitsi jos siitä ei todennäköisesti aiheudu riskiä luonnollisten henkilöiden oikeuksiin.
Lisäksi asetuksen 33 artiklassa luetellaan minimivaatimukset tiedoista, joita ilmoituksessa on oltava. (Tietosuoja-asetus 679/2016, artikla 33.)

Tietosuoja-asetus määrää myös ilmoittamisesta rekisteröidylle, mikäli tietoturvaloukkaus aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille. (Tietosuoja-asetus 679/2016, artikla 34.)

2.6 Tietoturva

Rekisterinpitäjän ja varsinkin rekisterinkäsittelijän on jo ennen asetuksen soveltamisen alkamista selvitettävä ja arvioitava, vastaavatko käytännöt henkilötietojen käsittelyssä asetuksen vaatimuksia. Mikäli arvioinnissa huomataan riskejä, on niitä vähennettävä huomioiden saatavilla oleva tekniikka ja kustannukset suhteessa tietojenkäsittelyn riskeihin ja henkilötietojen luonne. (Tietosuoja-asetus 679/2016, artikla 32.)

2.7 Keskeiset uudistukset aiempaan lainsäädäntöön verrattuna

Tuon tässä esiin mitä uutta tai huomattavasti muuttunutta tietosuoja-asetuksessa on verrattuna aiemmin julkaistun direktiivin pohjalta tehtyyn lainsäädäntöön.

- Henkilötietojen huolellinen säilyttäminen.
- Henkilötietojen keräämisen minimointi ja salaus.
- Järjestelmien toimintavarmuuden, käytettävyyden ja jatkuvuuden takaaminen ja järjestelmän palauttaminen nopeasti.
- Tietoturvaloukkauksista ilmoittaminen valvontaviranomaiselle ja rekisteröidylle.
- Tietojenkäsittelyn turvallisuuden varmistaminen, myös testaamalla.
- Tietosuojavastaavan nimeäminen tarvittaessa.
- Säädöksen laiminlyönneistä sanktiot.

3 Yrityksen esittely

Löysin toimeksiannon Haaga-Helian ammattikorkeakoulun MyNet verkkosivustoiden ”Aiheita toimeksiantajilta” sivulta. Siellä oli ilmoitus: ”Haemme Opinnäytetyöntekijää EU:n tietosuoja-asetus (GDPR)”. (Haaga-Helia 2018.) Koska olen kiinnostunut tietoturvasta ja tietosuojasta, otin yhteyttä ilmoituksen tietojen perusteella Yritykseen ja sovimme tapaamisen. Heti ensimmäisestä tapaamisesta lähtien tuntui siltä, ettei muualle tarvitse olla yhteydessä opinnäytetyön toimeksiannon kanssa, eikä heidän tarvitse etsiä toista tekijää. Sovimme toimeksiantosopimuksen ja NDA:n allekirjoittamisesta seuraavassa kokouksessa.

Yritys toimii ulkoistetun asiakashankinnan kilpaillulla toimialalla. Tämä tarkoittaa, että yritys sopii ennalta hankittujen tietojen perusteella tapaamisia toimeksiantajan puolesta. Yritys kuuluu Suomen suurimpiin omalla toimialallaan.

Yritys toimii pääosin rekisterinkäsittelijän roolissa. Sillä on myös rekisterinpitäjän rooli. Molemmissa rooleissa tietosuoja-asetuksen vaatimukset pitää luonnollisesti täyttää. Tämä toi alussa vaikeuksia hahmottaa, miten Yrityksen tulisi toimia eri tilanteissa, voidakseen täyttää tietosuoja-asetuksen vaatimukset. Suurin osa Yrityksen liiketoiminnasta tapahtuu rekisterinkäsittelijän roolissa. Tätä pohdittuani päätin Yrityksen kanssa lähestyä tietotilinpäätöstä riskiperusteista lähestymistapaa käyttäen, rekisterinkäsittelijän roolin ollessa ensisijaisena, tehdessäni tietotilinpäätöstä.

Tähän päätökseen vaikutti myös se, että henkilötiedot, joita Yritys käyttää sopiakseen tapaamisia eivät sisällä arkaluontoisia tietoja, kuten sosiaaliturvatunnusta, terveystietoja, poliittiseen vakaumukseen tai uskontoon liittyviä tietoja.

3.1 Suunnitelma

Ennakkoon olin ajatellut, että tekisin toimeksiannosta projektimuotoisen. Toimeksiannolla olisi silloin projektin mukaisia raameja, kuten aikataulu, vastuuhenkilöt, rajaukset. Tämä ei kuitenkaan toteutunut, muun muassa siksi, että Yrityksellä oli alussa suuri kiire saada työ aloitetuksi. Myöhemmin minulle selvisi, että tähän kiireeseen liittyi kolmas taho, joka vaati Yritykseltä tätä dokumenttia. Huolimatta Yritykselle muodostuneesta paineesta lähettää kolmannelle taholle keskeneräinen dokumentti, näin ei kuitenkaan menetelty.

Rekisteriselosteet, jotka ovat Yrityksen julkisilla verkkosivuilla kerättyjä, rajautuivat pois toimeksiannostani, koska niitä ylläpitää toinen taho.

4 Dokumentin luominen Yritykselle

Toimeksiannon mukainen tietotilinpäätöksen tekeminen alkoi marraskuussa 2017 ensimmäisen tapaamisemme jälkeen. Olin tutustunut tietosuoja-asetukseen jo ennen tapaamistamme, joten pääsimme heti työntekoon.

Toimintatavaksemme muotoutui tekemäni tietotilinpäätöksen kulloisenkin version läpikäynti ja muutoksista keskusteleminen.

4.1 Toteutus

Tietosuojatilinpäätös -dokumentin teon Yritykselle aloitin jo ennen ensimmäistä kokousta. Olin tutustunut löytämiini julkisiin tietotilinpäätöksiin, joita olivat Väestörekisterikeskuksen tietotilinpäätös 2016, Viestintäviraston tietotilinpäätös 2016 ja Trafi Tietotilinpäätös 2015. Vein kyseisten tietotilinpäätösten sisällysluettelot Excel-taulukkoon ja vertailin niitä. Näkymä Excel-taulukosta on kuvassa 1.

Trafi	VRK	Viestintä
1 Tietojohtajan katsaus	1. Johdanto	1 Johdanto
2 Johdanto	2. Tietojen käsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus	2 Tietojen käsittelyyn vaikuttava keskeinen säädäntö muuttumassa
3 Liikenne- ja viestintäministeriön hallinnonalan konse	2.1 Tietojen käsittelyä ohjaava ohjeistus	2.1 Sääntelyn sisällöstä pääpiirteittäin
3.1 Liikenne- ja viestintäministeriön hallinnonalan kon	2.2 Käytännesäännöt sekä rekisteri- ja tietosuojaselosteet	2.2 Rekisterinpitäjän vastuut ja velvoitteet
3.2 Trafin strategiset päämäärät	2.3 Toimintapolitiikat, ohjeet ja koulutus	2.2.1 Osoitusvelvollisuus
3.3 Tieto konsernistrategian ja Trafin strategisten pääm	3. Keskeisimmät tietovirrat ja tulovirrat	2.2.2 Sisäänrakennettu ja oletusarvoinen tietosuoja
4 Tiedon johtamisen lähtökohdat ja periaatteet	4. Käytettävyys	2.2.3 Tietoturvaloukkauksista ilmoittaminen
4.1 Keskeiset käsitteet	5 Väestötietojärjestelmän tietojen ylläpito	2.2.4 Henkilötietojen käsittelijä
4.2 Lainsäädännön viitekehys ja valtiokonsernin ohjaus	6 Väestötietojärjestelmän ja varmennetietojärjestelmän palve	2.2.5 Tietosuojavastaava
4.2.1 Hyvän tietojenkäsittelytavan ja hyvän tiedonhallir	7 Väestötietojärjestelmän tietojen luovutusten palvelukohtais	2.3 Rekisteröidyn oikeudet
4.3 Rekisterinpitäjän vastuut tietosuoja- ja tietoturvana	8 Kansalaisen tietojenluovutuskielto-oikeuden ja tietojen tarka	2.3.1 Oikeus saada tietoa henkilötietojen käsittelystä

Kuva 1. Näkymä sisällysluetteloista

Järjestin otsikot vastaamaan toisiaan niin hyvin kuin se oli mahdollista. Hyvin pian huomasin, että kyseisissä tietotilinpäätöksissä lähes kaikki tieto oli sellaista, jota en voisi käyttää hyväkseni toimeksiannossa. Tämä johtui siitä, että kyseiset organisaatiot toimivat niin erilaisella liiketoiminta-alueella ja ovat täysin eri kokoluokassa kuin toimeksiantajani. Nämä organisaatiot ovat myös viranomaisia, joiden toiminta perustuu lainsäädäntöön. Tämän huomion jälkeen poistin kaikki työni kannalta epäoleelliset otsikot ja järjestin ne uudelleen. Arvioin kyseisiä tietoja ja poimin niistä ne, joiden kuvittelin koskevan toimeksiantajaani. Näin sain ensimmäiseen kokoukseemme materiaalia, josta lähteä liikkeelle.

Aiemmin tutustuessani tietosuoja-asetuksen, olin lukenut myös riskiperusteisesta lähestymistavasta, jota ajattelin soveltaa sitä mahdollisuuksieni mukaan tehdessäni toimeksiantoa.

Ensimmäisessä kokouksessa ehdimme käydä läpi pääpiirteissään Yrityksen liiketoiminnan ja mitä sovelluksia ja käyttöjärjestelmiä heillä on käytössä. Esittelin tekemäni sisällysluettelon ja sovimme, että sitä voidaan käyttää tilinpäätöksen karkeana pohjana ja riskiperusteinen lähestymistapa sopi myös heille. Ihan aina en saanut suoraan vastausta kysymykseen tai he eivät osanneet suoralta kädeltä vastata. Lopuksi kuitenkin vastaukset löytyivät suurimpiin kysymyksiin.

Totesin, että yrityksellä on 3 rekisteriä, joista kaksi on julkisilla verkkosivuoilla. Toinen niistä on yrityksille tarkoitettu yhteydenottopyyntölomake ja toinen on yksityishenkilöille työpaikan hakemista varten. Kolmas on työntekijärekisteri. Kaikki muu toiminta, eli yrityksen liiketoiminta perustuu rekisterinkäsittelijän rooliin. Vaikka yrityksen liiketoiminnassa käyttämät henkilörekisterit ovat pääsääntöisesti käytössä vain lyhyen ajan toimittajien henkilörekistereistä, niin nämä kolme Yrityksen omaa rekisteriä vaikuttivat suuresti siihen, että tietotilinpäätöksessä huomioitiin myös rekisterinpitäjän näkökulma.

Toimittajien toimittamalla materiaalilla, tai Yrityksen toimeksiantona hankkimalla materiaalilla, on ennalta sovittu käyttöaika. Tämä tarkoittaa myös sitä, että Yrityksen kampanjoilla on sama, tai lyhyempi kesto. Tämä kampanjan kestoaika on tyypillisesti kaksi kuukautta. Käytännössä materiaalia kuitenkin joudutaan säilyttämään lähes poikkeuksetta pidempään siinä tapauksessa, että kohteen kanssa on sovittu uusi soittoaika kampanja-ajan ulkopuolelle. Toinen syy säilyttää tietoja hieman pidempään on kohteen bookkaus tai kohteen puhelun aikana tekemä markkinointi kielto. Jos kohde tekee markkinointi kiellon, niin kyseisen kohteen puhelinnumero viedään estolistaan. Bookkaus- tiedot säilytetään 12 kuukautta ja estolistan tiedot 60 kuukautta.

4.1.1 Haasteet toteutuksessa

Toteuttaessani tietotilinpäätöstä törmäsin usein ns. hiljaiseen tietoon, tai ainakin sen niin tulkitsin. Hiljainen tieto on henkilökohtaista, kokemukseen perustuvaa tietoa. En saanut luettavakseni mitään Yrityksen tekemää dokumenttia missään toimeksiannon tekemisen vaiheessa. Tämän vuoksi jouduin työstämään tietotilinpäätöstä omien keskusteluistamme tekemieni muistiinpanojeni pohjalta ja muistinvaraisesti. Sain luettavakseni Yrityksen toimittajien ja sovellustoimittajien dokumentaatiota, joita saatoin jossain määrin soveltaa työtä tehdessäni. Näitä dokumentteja en voi tähän laittaa liitteeksi, mutta erään sovellustoimittajan dokumentti oli heidän näkemys tietotilinpäätöksen tekemisestä. Sain tämän dokumentin luettavakseni vasta työni loppuvaiheessa, joten päätimme yhdessä, ettemme lähde muuttamaan tekemäni tietotilinpäätöksen rakennetta sen perusteella.

Suurena ongelmana työn jossain vaiheessa näin sen, että Yritys ei osannut vastata, miten toimittaja määrittelee rekisterimateriaalin käyttöajan, ja muut mahdolliset määräykset materiaalin käytön suhteen. Yritin selvittää sitä myös lähettämällä sähköpostia eräälle rekisterinpitäjälle. Vastauksena sain, että se on aina sovittu erikseen rekisterinpitäjän ja heidän asiakkaan välisessä sopimuksessa. Myöhemmin kuitenkin sain erään toimittajan toimittaman dokumentin luettavakseni, missä oli määritelty, miten heidän toimittamaansa rekisterimateriaalia tulee käsitellä. Sovimme, että otamme tämän mallin tietotilinpäätökseen, ja että yritys sitoutuu toimimaan sen ohjeiden mukaisesti, jollei se saa muita kirjallisia ohjeita toisilta toimittajilta.

Toinen merkittävä seikka oli se, ettei Yritys juurikaan puuttunut tietotilinpäätöksen rakenteeseen tai sisältöön muuten kuin teknisissä yksityiskohdissa.

Lisäksi Yrityksen toimintatavat kehittyivät läpi koko prosessin ajan, sitä mukaa, kun toisaalta he ymmärsivät, mitä uusia vaatimuksia tietosuoja-asetus Yritykselle määrittelee ja toisaalta mitä uudistettuja oikeuksia yksityishenkilöt saavat. Yrityksessä otettiin käyttöön uusia sovelluksia ja toimintatapoja sinä aikana, kun tein Yritykselle tietotilinpäätöstä.

4.2 Tuotos

Tuotoksena tein liitteenä olevan tietotilinpäätöksen. Käyn tiivistetysti läpi Yrityksen toiminta tavoissa tapahtuneita muutoksia, tai olivat mitkä työni kannalta muuten merkittäviä. Koska Yritys on pääsääntöisesti rekisterinkäsittelijä, niin tietotilinpäätöksessä tämä reksiterinkäsittelijän rooli korostuu.

4.2.1 Rekisteritietojen liikkuminen

Tietosuoja-asetuksen keskeinen seikka on henkilörekisterit, ja se mitä niihin on tallennettu. Koska Yritys on pääasiallisesti rekisterinkäyttäjä, minulle oli erityisen tärkeä ymmärtää miten Yritys näitä rekistereitä käyttää, ja miten ne Yritykselle tulevat. Jouduin työni aikana useasti palaamaan tähän seikkaan, ja varmistamaan miten tiedot kulkevat, koska tietojen toimitustavat muuttuivat toimeksiannon aikana.

Yritys voi saada liiketoiminnan kannalta tärkeät rekisteritiedot usealla eri tavalla. Käytännössä valtaosa Yrityksen käyttämästä henkilötiedoista joko toimitetaan Yritykseen toimittajan toimesta tai Yritys hankkii tiedon toimeksiantona.

Tässä on tarkasteltu rekisteritietojen kulkua näiden kahden pääasiallisen toimintatavan kannalta Yrityksen näkökulmasta, sekä miten Yritys toimittaa projektiraportin asiakkaalle.

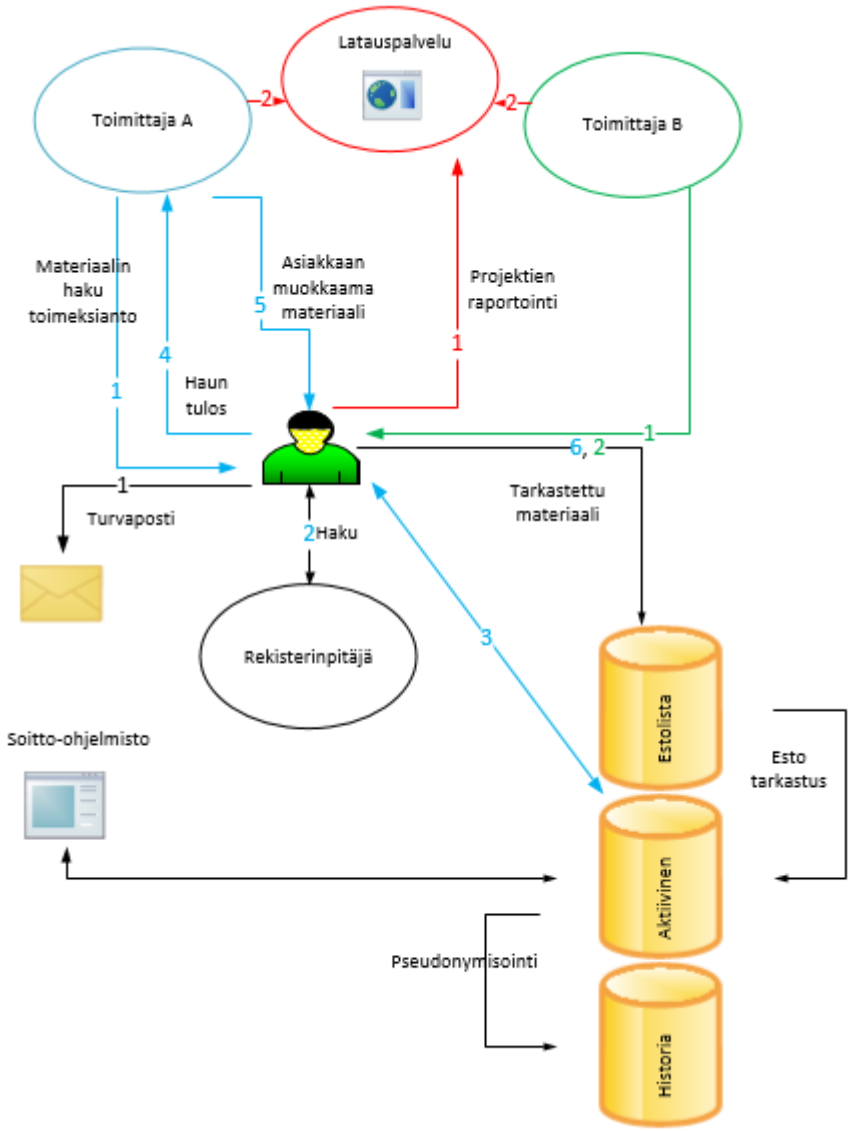
1. Toimittaja A tekee Yritykselle toimeksiannon, jossa se pyytää Yritystä hakemaan tietoja toimittaja A:n kanssa sopimalta rekisterinpitäjältä toimittajan A:n määrittelemin ehdoin.
2. Yritys hakee tiedot rekisterinpitäjältä.
3. Yritys vertaa niitä viimeisimpiin aktiivisiin tietoihin
4. Yritys lähettää ne toimittaja A:lle tarkistusta ja mahdollisia muutoksi / lisäyksiä varten.
5. Toimittaja A palauttaa materiaalin Yritykselle.
6. Yrityksen manuaalisen tarkistuksen jälkeen materiaalia verrataan estolistaan, jonka jälkeen materiaali menee tuotantoon.

1. Toimittaja B toimittaa rekisterimateriaalin.
2. Yrityksen manuaalisen tarkistuksen jälkeen materiaalia verrataan estolistaan, jonka jälkeen materiaali menee tuotantoon. Estolistaan kerätään sellaisten henkilöiden puhelunnumerot, jotka kontaktitilanteessa kieltävät markkinoinnin.

1. Yritys lataa Projektin raportin latauspalveluun.
2. Toimittaja hakee raportin latauspalvelusta.

1. Yrityksen joutuessa lähettämään rekisteritietoja sähköpostitse se käyttää Turvapostia.

Seuraavassa kuvassa esitetään rekisteritietojen pääasiallinen kulku Yrityksen ja toimittajan välillä.

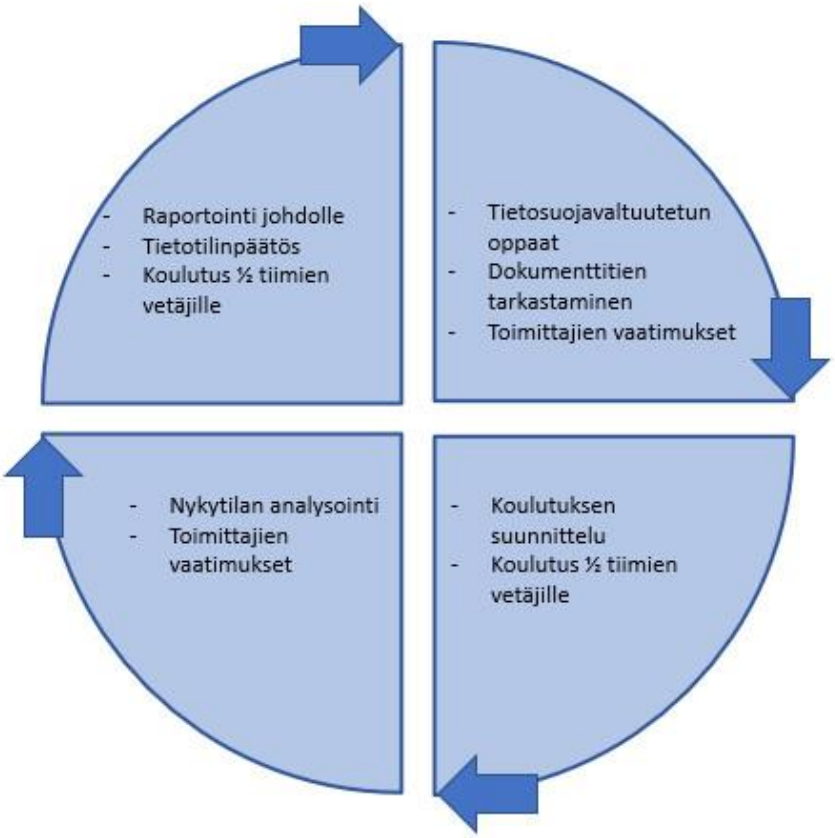


Kuva 2. Rekisteritietojen kulku

4.2.2 Tietosuojavuosikello

Vuosikello on yleisesti käytössä oleva yleensä graafinen työkalu, jolla suunnitellaan vuoden aikana tapahtuvat työt. Tein Yritykselle tietosuojavuosikellon, jonka avulla Yritys voi suunnitella vuosittaisen kvartaaleittain toistuvat tietosuojaan liittyvät asiat kuten tietosuoja tietämyksen ylläpidon, dokumentaation, raportoinnit, toimittajien vaatimukset ja koulutuksen.

Koulutuksella on suuri merkitys tietosuojavuosikellossa, koska yrityksessä on suuri vaihtuvuus henkilökunnassa.



4.2.3 Ristiintaulukointi

Koska suuri osa opinnäytetyöstä on toimeksiantona tekemässäni tietotilinpäätös -dokumentissa, tein taulukon, josta selviää missä kohdassa tietotilinpäätöstä eri tietosuoja-asetuksen kohtia on käsitelty.

Säädöksen asettamat oikeudet	Yrityksen toimintatapa	Kohta opinnäytetyössä	Liitteessä
Läpinäkyvä informaatio	Kerrotaan tietojen lähde kysyttäessä. Yrityksen julkisilla verkkosivuilla on rekisteriseloste.	2.2.1	8.1
Pääsy tietoihin	Vastaanotetaan pyyntö ja välitetään toimittajalle.	2.2.2	4.3 ja 8.2
Tietojen oikaisu ja unohtaminen	Vastaanotetaan pyyntö ja välitetään toimittajalle	2.2.3	4.3 ja 8.3
Rajoittaminen	Vastaanotetaan pyyntö ja välitetään toimittajalle	2.2.4	4.3 ja 8.3
Tietojen siirto	Vastaanotetaan pyyntö ja välitetään toimittajalle	2.2.5	4.3, 7 ja 8.4
Vastustaminen	Vastaanotetaan pyyntö ja välitetään toimittajalle	2.2.6.	8.4
Profilointi	Yritys ei tee profilointia	2.2.7	7.6
Säädöksen asettamat velvollisuudet	**Yrityksen toimintatapa**	**Kohta opinnäytetyössä**	**Kohdat dokumentissa**
Oletusarvoinen tietosuoja	Yritys on dokumentoinut toimintansa ja kouluttaa henkilökuntaansa sekä noudattaa toimittajilta saamiaan kirjallisia ohjeita.	2.3.1	3.3
Oikeusperusta	Yritys kerää ja käyttää ainoastaan tarpeellisia tietoja.	2.3.2	4 ja 7
Osoitusvelvollisuus	Yritys on dokumentoinut toimintatapansa ja kouluttaa henkilöstönsä.	2.3.3	3.3
Tietoturvan hallinta	Kaikki rekisteritietojen käsittelyvaiheet on pyritty tekemään tietoturvallisesti.	2.6	4
Tiedonanto ja yhteistyövelvoite	Ilmoitetaan tarvittaessa valvontaviranomaiselle	2.5	4.4
Tietoturva	Yritys huomioi tietoturvan kaikessa tietotekniikassa ja ohjelmistoissa	2.6	5.1

Taulukko 1. Ristiintaulukointi

4.3 Mikä muuttui

Kuten aiemmin jo mainitsin, moni asia muuttui Yrityksen toimintatavoissa tietotilinpäätöstä tehdessäni. Tämä vaikeutti tietotilinpäätöksen tekemistä, koska seurattavia ja muutettavia asioita oli useita saman aikaisesti.

Rekisteritietojen siirtämisessä Yritykseltä toimittajalle siirryttiin käyttämään operaattorin tarjoamaa palvelua, Turvapostia aina, kun se on mahdollista. Palvelussa viestit salataan ja käyttäjä tunnistautuu kertakäyttöisellä salasanalla.

Yritys tilasi latauspalvelun, jonka avulla toimittaja toimittaa rekisteritiedot yritykselle. Se on tietoturvallinen verkkosivu, jossa käyttäjä tunnistetaan.

Kampanjamateriaalien tietojen poistoon tuli selkeämpi toimintatapa ja nauhoitettujen puheluiden käyttöoikeuksia rajoitettiin koskemaan ainoastaan kulloisenkin projektin tekijöille. Näiden tietojen säilyttämiselle määriteltiin tarkat säilytysajat kuukausina.

Yritys tarkensi ohjeistustaan tiimien vetäjille ja loppukäyttäjille. Näitä dokumentteja en kuitenkaan nähnyt.

Projekteille luotiin uusi kansiorakenne, johon tarkennetut ohjeet työntekijöille lisättiin. Kansioiden käyttöoikeudet tarkastettiin samalla.

Julkisille verkkosivuille tuli päivitetty, helposti löydettävissä oleva rekisteriseloste toisen osapuolen toimesta.

5 Pohdinta ja johtopäätelmät

Opinnäytetyönäni oli tehdä EU:n tietosuoja-asetuksen 2016/679 mukainen tietotilinpäätös työn tilanneelle yritykselle. Minulla ei ollut ennakkoon mitään tietoa kyseisestä yrityksestä, eikä tuntemusta sen toimialasta. Vaikka tietotilinpäätöksiä oli vapaasti verkosta luettavissa niistä ei ollut juurikaan apua työhöni, koska nämä eivät yritysten koon ja luonteen vuoksi olleet mitenkään rinnastettavissa yritykseen, jolle tilinpäätöksen tein. Tämän vuoksi jouduin tehdä työn ilman esimerkkien mahdollisesti antamia sisällöllisiä vihjeitä.

Aloitettuani työni tutustuin syvällisemmin aiheeseen etsimällä internetistä aiheeseen liittyvää materiaalia ja ohjeita tietotilinpäätöksen tekemiseksi. Lehtiartikkeleissa huomasin puutteita yksityiskohdista ja virheitä. Yleisimmin löytämäni virhe liittyi asetuksen voimaan tulemiseen, joka oli usein määritelty 25.5.2018, vaikka tuo päivämäärä on se, jolloin asetusta aletaan soveltamaan. Suureksi avuksi työssäni oli Oikeusministeriön julkaisu 4/2017: ”Miten valmistautua EU:n tietosuoja-asetukseen?”. Siitä sain asiasisältöä työhöni ja saatoin käyttää sitä osaltaan vertaamaan, olenko huomioinut kaikki oleelliset asiat työssäni. Toki suurin ohjeeni oli asetus itse.

Suurimmaksi haasteeksi työssäni muodostui tietosuoja-asetuksen rakenne, joka ei ole selkeä, kronologinen tai helposti lähestyttävä. Artikloissa asiat on esitetty viittaamalla toisiin artikloihin ja niiden kohtiin. Esimerkkinä voin ottaa tietosuoja-asetuksen 12 artiklan kohdan 1, jossa viitataan yhdeksään muuhun artiklaan. Jos koko asetusta ei osaa ulkoa, asioiden selvittäminen vaatii jatkuvaa asetuksen selausta. Säädös on laaja, koskettaa kaikkia ja siinä on pyritty huomioimaan kaikki eri vaihtoehdot, joka osaltaan selittää asetuksen rakenteen. Termistökin jää osittain epäselväksi, kuten esimerkiksi termi pseudonymisointi, jota asetuksessa on yritetty selvittää, mutta mielestäni huonolla menestyksellä:

> ”’pseudonymisoimisella’ henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu.”. (Tietosuoja-asetus 679/2016 artikla 4.)

Toinen merkittävä haaste oli se, ettei Yritys juurikaan puuttunut tietotilinpäätöksen rakenteeseen tai sisältöön muuten kuin teknisissä yksityiskohdissa. Tämä saattoi johtua yrityksen opinnäytetyöhöni osallistuneiden henkilöiden työkuormasta tai siitä, että jotkut asiat eivät olleet heidän työnsä kannalta merkittäviä tai heidän vaikutusvaltansa piirissä. Olisin

toivonut heiltä aktiivisempaa otetta tekemäni tietotilinpäätöksen rakentavan kritiikin antamisessa tai vielä ponnekkaampaa osallistumista sen sisältöön.

Työssäni olen aiemmin kertonut asioista, jotka yrityksessä muuttuivat työni aikana. Mielestäni yritykseen jäi vielä asioita, jotka eivät muuttuneet, vaikka niiden olisi pitänyt. Yrityksen itse tuottaman dokumentaation puuttuminen vaivasi minua koko ajan, kun tein tietotilinpäätöstä, vaikka painotin sen tärkeyttä osaltaan asetuksen vaatiman osoitusvelvollisuuden täyttämisessä ja osaltaan yrityksen yleisen edun nimissä.

En päässyt osallistuman tiimien vetäjien pitämiin koulutuksiin uusille työtekijöille, enkä nähnyt koulutusmateriaalia, joten en osaa arvioida, kuinka suuri osuus tietosuoja asioissa niissä on. En nähnyt tai osallistunut yrityksen päivittäiseen työhön, vaikka yritimme sellaista järjestää, joten kaikki yrityksen varsinaiseen työhön liittyvät toimintamallit ja -tavat sain tietooni yrityksen työhön osallistuneiden henkilöiden kertomana.

Kyseenalaistamalla heidän nykyisiä toiminta tapojaan sain heidät pohtimaan niitä. Tämän ansiosta sain toisista toiminnoista yksityiskohtaisempaa tietoa, jota pystyin hyödyntämään työssäni. Uskon tämän vaikuttaneen myös heidän toimintansa kehittymiseen tietosuoja-asetuksen vaatimusten mukaiseksi.

Tietosuoja-asetuksessa on paljon hyviä parannuksia sitä edeltäneeseen tilanteeseen verrattuna. Sen ansiosta mm. henkilörekisterien tietojen käytön läpinäkyvyys lisääntyy ja rekisteritiedot ovat rekisterinpitäjillä paremmin suojattuna. Asetuksessa on otettu huomioon tietojen arkaluonteisuuden ja tietojen suojaamisesta aiheutuvien kustannusten suhde, joka helpottaa pieniä ja keskisuuria yrityksiä selviytymään asetuksen vaatimista muutoksista. Näen tämän kokoisten yritysten joutuvan liian suuren työtaakan alle, selvittäessään asetusten vaatimusten ja oikeuksien toteuttamisen käytännössä, varsinkin, jos niiden tietosuoja on jo ollut riittävällä tasolla. Useinkaan näillä yrityksillä ei ole mahdollisuutta varata resurssia pelkästään asetuksen vaatimusten tarkastamiseen ja seuraamiseen.

5.1 Oman oppimisen arviointi

Ennen työn aloittamista olin tutustunut EU:n tietosuoja-asetukseen, ja luulin omaavani siitä jonkinlaisen käsityksen. Työni edetessä huomasin, että en ollut oikeasti tiennyt asetuksesta syvällisesti paljoakaan. Jouduin usein jäsentämään ja miettimään asiat uudelleen ymmärrykseni asetuksen vaatimuksista lisääntyessä.

Tietotilinpäätöstä tehdessäni tutustuin tietosuoja-asetukseen pääosin vain yrityksen näkökulmasta oppimisen painottuessa rekisterinkäsittelijän näkökulmaan, vaikka pieneltä osin otinkin rekisterinpitäjän pieneltä osin asioita huomioon. Näitä kahta roolia ei mielestäni voi täysin eriyttää yrityksen näkökulmasta. Näin ollen minulta jäi vielä perehtymättä osaan säädöksen asioista.

Jos tulisi tilanne, että tekisin uudelleen tietotilinpäätöksen jollekin taholle, tekisin sen hieman eri tavalla. Toisin kuin nyt, tekisin ensin tietotilinpäätökseen rungon säädöksen asettamista velvollisuuksista rekisterinpitäjälle tai rekisterinkäsittelijälle ja rekisteröidyn oikeuksista ja sitten vertaisin niitä tietotilinpäätöksen tarvitsijan nykyiseen toimintaan.

Vaikka Yritykselle tekemästäni tietotilinpäätöksestä puuttuu muutama lähipäivinä tapahtuvien muutosten huomioiminen, niin uskon, että se auttaa yritystä selviytymään asetuksen osoitusvelvollisuudesta.

Lähteet

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017:35.

Euroopan Parlamentin ja neuvoston asetus (EU) 2016/679. Yleinen tietosuoja-asetus. Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI. Luettu: 28.12.2017.

Finlex 2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Luettavissa: https://www.finlex.fi/fi/esitykset/he/2018/20180009. Luettu: 22.3.2018.

Haaga-Helia ammattikorkeakoulu 2018. MyNet. Intranet. Aiheita toimeksiantajilta. Luettu: 26.11.2017

Laine, L. 2018. Kohu käyttäjien tiedoista. Helsingin Sanomat, 78 (42768), s. 21.

Oikeusministeriö 2016. Henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistaminen (TATTI -työryhmä). Luettavissa: http://oikeusministerio.fi/hare?selectedProjectId=17607. Luettu: 13.2.2018.

Oikeusministeriö 2017, Tietosuojavaltuutetun toimisto. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017. Anu Talus, oikeusministeriö ja Elina Autio, Anna Hänninen, Heljä-Tuulia Pihamaa ja Silja Kantonen, tietosuojavaltuutetun toimisto. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Luettu: 12.12.2017.

Trafi Tietotilinpäätös 2015. Luettavissa: https://www.trafi.fi/filebank/a/1463394812/9478dbd63f9d555bc3cd6f5b5bc99e54/20667-Trafin_julkaisuja_14-2016_-_Tietotilinpaatos_2015.pdf. Luettu: 1.12.2017

Viestintäviraston tietotilinpäätös 2016. Luettavissa: https://www.viestintavirasto.fi/attachments/Viestintaviraston_tietotilinpaatos_2016.pdf. Luettu: 1.12.2017

Väestörekisterikeskus 2018. Tietojen luovutuksen kieltäminen. Luettavissa: http://vrk.fi/vaestotietojarjestelma/tietojen-luovutuksen-kieltaminen. Luettu: 30.01.2018.

VÄESTÖREKISTERIKESKUKSEN TIETOTILINPÄÄTÖS 2016 Tiivistelmä. Luettavissa: http://vrk.fi/documents/2252790/2783772/Tietotilinp%C3%A4%C3%A4t%C3%B6s+2016+tiivistelm%C3%A4/b60e4c57-1a06-4503-84a4-96cd260d8f0d/Tietotilinp%C3%A4%C3%A4t%C3%B6s+2016+tiivistelm%C3%A4.pdf. Luettu: 31.11.2017

Liitteet

Liite 1. Tietotilinpäätös

Sisällysluettelo

1 Johdanto 26
2 Termistö 26
3 Tietojen käsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus 27
3.1 Tietojen käsittelyä ohjaava ohjeistus 27
3.2 Rekisteri- ja tietosuojaselosteet 28
3.3 Toimintapolitiikat, ohjeet ja koulutus 28
4 Rekisteritietojen käsittely 29
4.1 Kampanjamateriaalit 29
4.2 Rekisteritietojen liikkuminen 29
4.3 Kampanjan tulosten toimittaminen Toimeksiantajalle 31
4.4 Muut rekisterit 31
4.5 Tiedonanto ja yhteistyö viranomaisten kanssa 31
4.6 Asiakastietojärjestelmän tietojen luovutus 32
5 Tietojenkäsittely ja järjestelmäarkkitehtuuri 32
5.1 Tietoturvan toteutuminen Yrityksessä 32
5.2 Järjestelmien arkkitehtuuri 32
5.3 Järjestelmien käyttövaltuudet 32
6 Järjestelmien ylläpito ja ylläpitotapahtumien seuranta ja valvonta 33
6.1 Järjestelmätoimittajien ja yhteistyökumppaneiden käyttöoikeudet 34
7 Asiakkaiden tekemä tietojenluovutuskielto ja tietojen tarkastusoikeuden toteutuminen 34
7.1 Oikeus saada tietoa henkilötietojen käsittelystä 34
7.2 Oikeus saada pääsy tietoihin 34
7.3 Oikeus tietojen oikaisemiseen ja tulla unohdetuksi 34
7.4 Tietojen siirto 34
7.5 Vastustamisoikeus 34
7.6 Automatisoidut yksittäispäätökset ja profilointi 35
8 Tehdyt kehittämistoimenpiteet ja havaitut kehittämiskohteet 35
8.1 Kehittämiskohteiden seuranta 35

1 Johdanto

Tämä on Yrityksen ensimmäinen tietotilinpäätös. Sen tehtävänä on osoittaa, että Yritys noudattaa toukokuussa 2018 sovellettavaksi tulevan yleisen tietosuoja-asetuksen mukaista tilintekovelvollisuus -periaatetta. Tätä tietotilinpäätöstä tehtäessä on Yrityksen toiminta tarkoin kartoitettu, jotta voidaan todentaa Yrityksen toimivan uuden tietosuoja-asetuksen mukaisesti.

Tietotilinpäätös on tarkoitettu ensisijaisesti Yritykselle sen toiminnan suunnitteluun erityisesti tietosuojan kannalta. Tietotilinpäätöksellä halutaan osoittaa, että tietojenkäsittelyn lainmukaisuus ja yleinen tietoturva on Yritykselle tärkeää ja se antaa yleiskuvan näiden toteutumisesta Yrityksessä. Tietosuojan sekä tietoturvan seuranta ja kehittäminen on Yrityksessä keskeisessä asemassa kuten myös sisäinen ja ulkoinen valvonta. Ulkoista valvontaa tapahtuu Toimeksiantajien taholta.

Yritys pyrkii kaikin tavoin lisäämään henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. Tämä koetaan erityisen tärkeäksi varsinkin nyt, kun Yritys on laajentanut toimintaansa Euroopan Unionin sisällä Suomen ulkopuolelle toiseen jäsenvaltioon. Vaikka Yritys ei itse aktiivisesti kerää tietoja, niin yrityksen prosessien läpi virtaavissa tiedoissa on henkilöitä yksilöiviä tietoja. Yrityksessä on dokumentoitujen seikkojen lisäksi ns. hiljaista tietoa rekisterien käsittelystä ja tietoturvaan liittyvistä asioista, jotka dokumentoidaan ja saatetaan tiedoksi Yrityksen sisällä. Näin saadaan kattava ohjeistus myös Yrityksen eri toiminteissa toimiville työntekijöille.

Yrityksen keräämä rekisteritiedot, toimiala tai laajuus eivät täytä tietosuoja-asetuksen tietosuojavastaavan nimeämisvelvoitetta. Siksi Yritys on päättänyt olla nimeämättä tietosuojavastaavaa. Tästä huolimatta Yritys on määritellyt tahon (henkilön) joka vastaa Yrityksessä tietosuojaa koskevien asioiden huomioon ottamisesta ja joka toimii yhteyspisteenä rekisteröidyn oikeuksiin ja viranomaisvalvontaan liittyvissä kysymyksissä.

2 Termistö

Alla olevassa taulukossa on kuvattu tässä dokumentissa käytettyjä termejä.

AD	Active Directory (aktiivihakemisto), hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.
Kohde	On henkilö tai yritys jolle buukkaaja soittaa
Boosteri	Selainpohjainen soitto- ja kalenterijärjestelmä.
Buukkaus	Kohde, jolle sovittu tapaaminen.
Domain	Toimialue, joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta tai työasemalta.
GP	Group Policy (ryhmäkäytäntö), keskitetysti AD:n kautta käytettävä hallintatyökalu.
GPO	Group Policy Object, ryhmäkäytännöillä tehdyt määrittelyt

	tallentuvat ryhmäkäytäntöobjekteiksi.
Hakemuslomake	Tietojenkeruu lomake Yrityksen julkisilla verkkosivuilla työpaikan hakemista varten.
HTTPS	Suojattu selaimella tapahtuva liikenne.
Kampanja	Projektiin liittyvä kohderyhmä / soittokausi.
Kohderyhmä	Henkilöt, joille soitetaan
Kontakti	Buukatut ja kieltäytyneet asiakkaat.
Käyttäjä	Yrityksen työntekijä.
Latauspalvelu	Tunnistautumista vaativa suljettu verkkopalvelu kampanjan tietojen siirtoa varten.
Lead Desk	Soittojärjestelmä, puhelin
MessageLock™	Sähköpostin salausmenetelmä.
PIN koodi	Personal Identification number, salasanana käytettävä luku, jolla voidaan tunnistautua järjestelmään.
Projekti	Asiakassuhde / asiakkuus.
SFTP	SSH File Transfer Protocol, salattu tiedostonsiirtomenetelmä.
SSH	Secure Shell, salatun tietoliikenteen protokolla.
VPN	Virtual Private Network, tekniikka jolla yhdistetään käyttäjä Yrityksen verkkoon Yrityksen ulkopuolelta. Yhteys on aina salattu.
Toimittaja	Yritys, joka toimittaa kohderyhmät Kampanjaan.
Turvaposti	Yrityksen käytössä oleva palvelu, joka mahdollistaa viestien lähettämisen ja vastaanottamisen tietoturvallisesti.

Taulukko 2, Termistö

3 Tietojen käsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus

Yrityksessä noudatetaan yksityisyyden suojaa, sananvapautta ja julkisuutta koskevia perusoikeussäännöksiä. Tätä tietotilinpäätöstä tehtäessä on voimassa henkilötietolaki (523/199), jota Yritys noudattaa. Tämä tietotilinpäätös on tehty huomioiden EU:n tietosuoja-asetuksen GDPR 2016/679 vaatimuksia.

3.1 Tietojen käsittelyä ohjaava ohjeistus

Yrityksen henkilöstöä ja yhteistyökumppaneita ohjataan tietojenkäsittelyssä dokumentoiduilla ohjeilla ja käytännesäännöillä. Samoin Yritys noudattaa Toimittajilta saamiaan kirjallisia asiakasrekistereihin liittyviä toimintaohjeita. Mikäli joku Toimittajista ei toimita ohjeita, niin Yritys soveltaa näihin muiden Toimittajien antamia käsittelysääntöjä.

3.2 Rekisteri- ja tietosuojaselosteet

Yrityksen julkisella verkkosivustolla on tietosuojaseloste, jota päivitetään lakien tai asetusten muuttuessa. Tämä tietosuojaseloste koskee ainoastaan Yrityksen julkisella verkkosivustolla kerättyjä tietoja.

3.3 Toimintapolitiikat, ohjeet ja koulutus

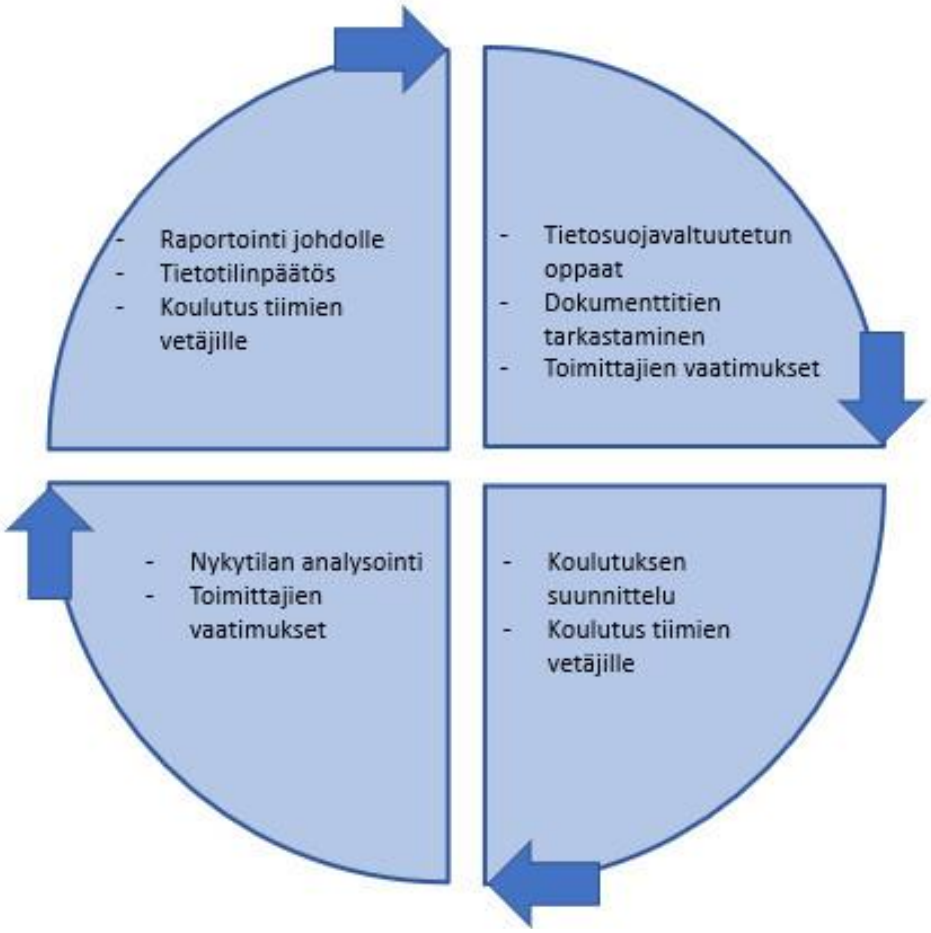
Yrityksessä järjestetään uusille henkilöille koulutusta tietoturva- ja tietosuoja asioista työhön perehdytyksen yhteydessä ryhmänjohtajien toimesta. Ryhmänjohtajat saavat säännöllistä vuotuista koulutusta tietoturva- ja tietosuojatietoisuuden ylläpitämiseksi ja lisäämiseksi. Koulutuksen sisältöä kehitetään ja ylläpidetään säännöllisesti. Tarvittaessa koulutusohjeita ja materiaaleja päivitetään uuden projektin alkaessa.

Nykyiselle henkilöstölle pidetään tietosuoja tietoisku, jossa kerrotaan, mitä muutoksia uusi tietosuoja-asetus tuo yrityksen toimintaan.

Yrityksessä ylläpidetään tietämystä tietosuojaasioista ja tarvittaessa päivitetään ja korjataan Yrityksen dokumentaatiota. Tietämyksen ylläpito tapahtuu pääasiassa seuraamalla säännöllisesti Tietosuojavaltuutetun toimiston sähköisiä tiedotteita ja uutisia osoitteessa http://www.tietosuoja.fi/fi/index.html.

Tietosuojavuosikellon avulla Yritys suunnittelee vuosittaiset kvartaaleittain toistuvat tietosuojaan liittyvät asiat, kuten tietosuoja tietämyksen ylläpidon, dokumentaation, raportoinnit ja Toimittajien vaatimukset.

Koulutus näyttelee suurta roolia tietosuoja vuosikellossa, koska Yrityksessä on suuri vaihtuvuus henkilökunnassa.



Kuva 3 Tietosuojavuosikello

4 Rekisteritietojen käsittely

Yritys ottaa tietoturvan huomioon kaikessa henkilötietojen käsittelyssä, ja on minimoinut Toimeksiantajien kanssa operoivien henkilöiden lukumäärän. Kaikki materiaali lähetetään ja vastaanotetaan suojattuja ja salattuja viestintävälineitä käyttäen aina, kun se on mahdollista.

4.1 Kampanjamateriaalit

Toimittajat toimittavat yritykselle tai Yritys Toimittajan toimeksi antamana hankkii kampanjaan kuuluvan materiaalin. Materiaali toimitetaan pääsääntöisesti sähköpostilla. Yritys poistaa tiedoista tarvittaessa ylimääräiset tiedot, eikä lisää mitään tietoja, ennen kuin ne siirretään aktiiviseksi projektiin. Yritys on tilannut latauspalvelun, joka korvaa materiaalin toimittamisen sähköpostitse. Latauspalvelussa on verkkosivu, jonka kautta projektien materiaalit siirretään Yritykselle Toimittajalta. Verkkosivulla on pakollinen sisäänkirjautuminen.

Tietoja käytetään kertaluonteisesti kyseessä olevaan projektiin, jonka jälkeen niiden henkilöiden henkilötiedot, joihin ei oltu yhteydessä, poistetaan järjestelmästä välittömästi, ellei Toimittaja ole antanut muunlaisia kirjallisia toimintaohjeita.

Onnistuneiden kontaktien tietoja säilytetään lukukelpoisina 12 kuukautta Toimeksiantajille tehtävää raportointia varten, jonka jälkeen ne anomynisoidaan, eli ylikirjoitetaan muotoon, josta tietoa ei voi kohdistaa luonnolliseen henkilöön. Täten yritykselle jää vielä mahdollisuus käyttää tietoa historiatietona.

Yrityksellä on sisäisesti käytössä oleva sulkulista. Tähän listaan kerätään henkilön nimi ja puhelinnumero siinä tapauksessa, että kontakti puhelun yhteydessä kieltää Yritystä ottamasta häneen yhteyttä tai kertoo voimassaolevasta markkinointikiellosta. Sulkulistalta poistetaan tiedot, jotka ovat 60 kuukautta vanhoja tai sitä vanhempia.

4.2 Rekisteritietojen liikkuminen

Yritys voi saada rekisteritietoja usealla eri tavalla. Tässä on tarkasteltu rekisteritietojen kulkua kahden pääasiallisen toimintatavan kannalta Yrityksen näkökulmasta, sekä miten Yritys toimittaa Projekti raportin asiakkaalle.

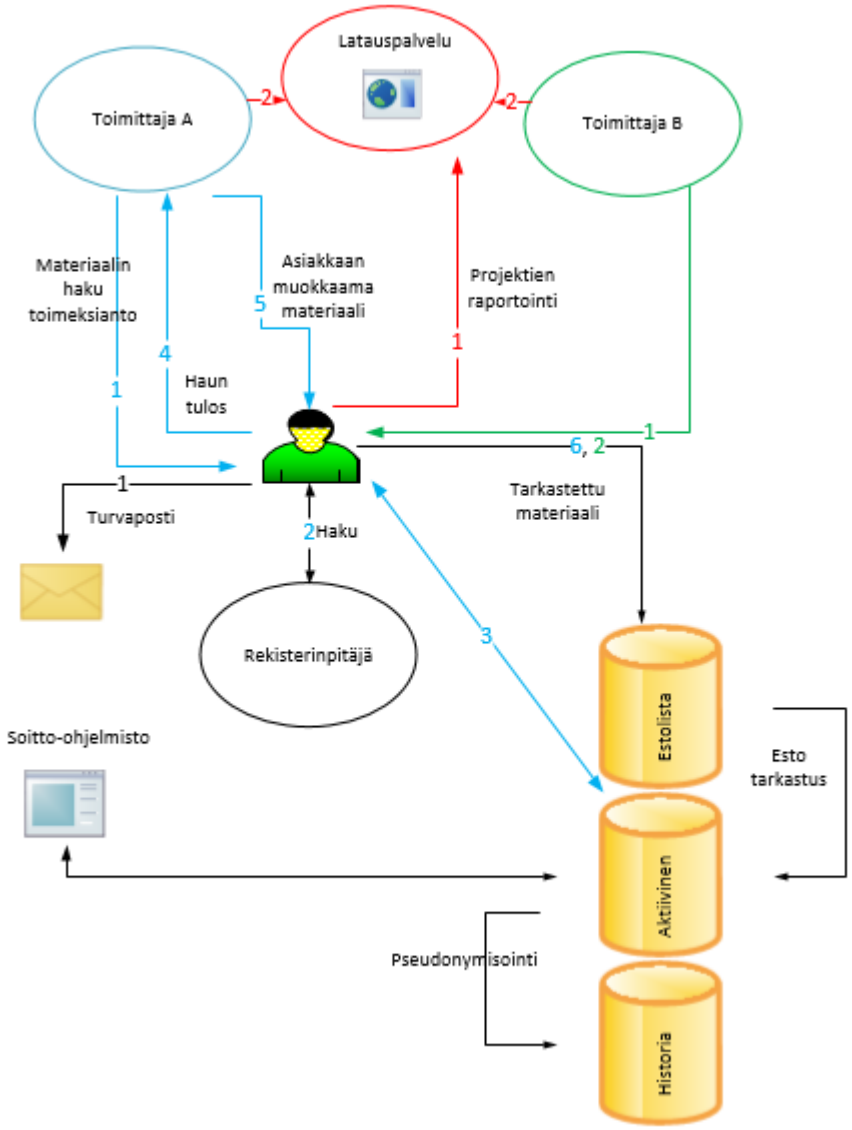
1. Toimittaja A tekee Yritykselle toimeksiannon, jossa se pyytää Yritystä hakemaan tietoja Toimittaja A:n kanssa sopimalta rekisterinpitäjältä Toimittajan A:n määrittelemin ehdoin.
2. Yritys hakee tiedot rekisterinpitäjältä.
3. Yritys vertaa niitä viimeisimpiin aktiivisiin tietoihin
4. Yritys lähettää ne Toimittaja A:lle tarkistusta ja mahdollisia muutoksia / lisäyksiä varten.
5. Toimittaja A palauttaa materiaalin Yritykselle.

6. Yrityksen manuaalisen tarkistuksen jälkeen materiaalia verrataan estolistaan, jonka jälkeen materiaali menee tuotantoon.

1. Toimittaja B toimittaa rekisterimateriaalin.
2. Yrityksen manuaalisen tarkistuksen jälkeen materiaalia verrataan estolistaan, jonka jälkeen materiaali menee tuotantoon.

1. Yritys lataa Projektin raportin Latauspalveluun.
2. Toimittaja hakee raportin Latauspalvelusta.

1. Yrityksen joutuessa lähettämään rekisteritietoja sähköpostitse se käyttää Turvapostia.



Kuva 4 Rekisteritiedon kulku

4.3 Kampanjan tulosten toimittaminen Toimeksiantajalle

Pääsääntöisesti kampanjan tulokset lähetetään Toimeksiantajalle Turvaposti-palvelun välityksellä.

”Turvaposti mahdollistaa viestien turvallisen lähettämisen sekä vastausviestin vastaanottamisen luottamuksellisesti mihin tahansa sähköpostiosoitteeseen. Käyttäminen ei vaadi työasemille asennettavia ohjelmia lähettäjällä eikä vastaanottajalla. Turvaposti muuntaa sähköpostiviestin www-selaimella luettavaan muotoon, tallentaa salatun viestin tilapäisesti järjestelmään ja lähettää vastaanottajalle ilmoitusviestillä suojatun linkin, jonka avulla varsinainen viesti voidaan avata”

Turvaposti- palvelussa on kaksi suojaustasoa, ”kirje” ja ”kirjattu kirje”, jotka vastaavat perinteisen postin vastaavia menetelmiä.

”Kirje” -tasolla viestit SSL salataan automaattisesti MessageLock™ -tekniikalla, jolloin viestin avaaminen on rajoitettu.

”Kirjattu kirje” -tasolla sähköpostin lisäksi samanaikaisesti lähetetään vastaanottajalle kertakäyttöinen PIN-koodi tekstiviestinä, mitä tarvitaan viestin avaamiseen.

4.4 Muut rekisterit

Yrityksellä on olemassa rekisteri työntekijöistä, HR- järjestelmä. Jokainen työntekijä pääsee näkemään omat tietonsa ja tiiminvetäjä näkee tiiminsä henkilöiden kaikki tiedot. Palkanhallinnassa nähdään myös kaikkien kaikki tiedot. Tätä ylläpidetään HR henkilöiden toimesta.

Julkisilla verkkosivuilla Yritys kerää yhteystietoja myynnin ulkoistamisesta kiinnostuneista tahoista. Lisäksi työpaikasta Yrityksessä kiinnostuneella henkilöllä on mahdollisuus täyttää pikahakemuslomake. Julkisilla verkkosivuilla on rekisteriseloste.

Mikäli henkilö antaa verkkolomakkeella yhteystietonsa ja haluaa

- saada pääsyn tietoihinsa
- oikaista tietojaan
- tulla unohdetuksi
- siirtää tietonsa
- vastustaa tietojen poistoa

niin Yritys toimii rekisteriselosteessa mainitulla tavoilla.

4.5 Tiedonanto ja yhteistyö viranomaisten kanssa

Mikäli Yrityksessä huomataan tietoturvaloukkaus, niin syyt siihen pyritään selvittämään ja korjaamaan huomatut virheet tai puutteelliset käytännöt. Syitä selvitetään eristämällä havainto, erilaisilla tietoturvaskannauksilla ja lokien analysoinnilla.

Tarvittaessa asiasta raportoidaan asianomaiselle valvontaviranomaiselle.

4.6 Asiakastietojärjestelmän tietojen luovutus

Toimittajilta ja julkisilla verkkosivuilla kerättyjä henkilötietoja käytetään ainoastaan siinä tarkoituksessa, mihin ne on kerätty. Yritys ei myy, luovuta tai vuokraa saamiaan henkilötietoja eteenpäin kolmansille osapuolille.

5 Tietojenkäsittely ja järjestelmäarkkitehtuuri

Yrityksen tietojenkäsittelyssä on järjestelmällisesti huomioitu tietoturvan ja -suojan vaatimukset.

5.1 Tietoturvan toteutuminen Yrityksessä

Yrityksen sisäverkko on palomuurein eristetty internetistä. Kaikissa Yrityksen työasemissa ja palvelimissa on virustorjunta- ja palomuuriohjelmistot käytössä. Yritys päivittää työasemiin ja palvelimiin käyttöjärjestelmäpäivitykset ja virustunnisteet säännöllisesti ja valvoo näiden päivitysten onnistumista. Lisäksi Yritys seuraa laitteistojen ja sovellusten valmistajien julkaisemia päivityksiä ja päivittää ne tarvittaessa. Kaikkien työasemien ja palvelimien tilanteen päivitysten suhteen Yritys näkee keskitetyn hallintakonsolin kautta.

Yrityksen sisäverkkoon ei saa kytkeä tietokonetta ilman yrityksen lupaa. Yrityksen palvelimet ja reitittimet sijaitsevat Yrityksen tiloissa lukitussa huoneessa.

Yrityksen tiloihin ei pääse ilman kulkukorttia. Vieraat ilmoittautuvat rakennuksen aulassa, josta heidät noudetaan Yrityksen tiloihin. Tiloissa on myös kameravalvonta.

5.2 Järjestelmien arkkitehtuuri

Yrityksellä on käytössään Windows 2012 toimialue, jolla hallitaan palvelimien, käyttäjien ja työasemien oikeuksia. Lisäksi yrityksellä on Linux palvelimia sovelluspalvelimina. Windows palvelimilla on rooleinaan AD:n lisäksi IIS ja levyjako palvelut. Nämä palvelut on asennettu Microsoftin ohjeiden ja yleisten hyvien käytäntöjen mukaisesti. Yritys käyttää toimistosovelluksena Office 365 ohjelmistoa, jonka saa käyttöön asentamalla sen Yrityksen palvelimelta. Ohjelmiston voi asentaa, kun on saanut käyttöönsä Yrityksen sähköpostitunnuksen. Sähköpostitunnus on muotoa etunimi.sukunimi@yritys.fi.

5.3 Järjestelmien käyttövaltuudet

Käyttäjät liitetään käyttäjäryhmiin, joilla annetaan oikeudet järjestelmiin ja tiedostoihin. Myös käytössä oleva työasema on liitettävä toimialueeseen, jotta se voisi toimia oikein.

Käyttäjäryhmien kuvaus

Johto	Yrityksen johdon henkilöt.
Administrators	Tämän ryhmän jäsenillä on pääsy kaikkialle toimialueella.
Tiiminvetäjät	Projektin vetäjät.
Projekti	Projektikohtainen ryhmä, jolla on pääsy projektien kansioihin ja resursseihin.
Users	Järjestelmä liittää kaikki käyttäjät tähän ryhmään automaattisesti.

Taulukko 3, Ryhmien kuvaus

Yrityksen IT-osastolla on hallinnassa kaikki yrityksen järjestelmien käyttövaltuuksiin liittyvät toiminteet. Käyttäjienhallinta (luonti, muutos ja poisto) on toteutettu Microsoft toimialueen Active Directoryssä. Käyttöoikeudet järjestelmiin ja kansioihin on toteutettu Windows ryhmäkäytänteillä (Group Policy). Jokaiselle projektille luodaan oma käyttöoikeusryhmä, jolla annetaan pääsyoikeus ko. projektin tietoihin. Käyttäjä liitetään jäseneksi tähän projektille luotuun käyttöoikeusryhmään, jolloin hänellä ei ole pääsyä muihin projektitietoihin. Käyttäjälle näkyy ainoastaan soittohetkellä järjestelmän esiin tuomat tiedot yksittäisestä kohteesta. Tiiminvetäjä näkee koko projektin sovitut tapaamiset raportoinnin kautta.

Samoin GP:llä on määritelty asetus, että peruskäyttäjällä ei ole oikeutta asentaa mitään (ohjelmaa) käyttämälleen työasemalle.

Lead Deskiin pääsyä on rajoitettu ip- suodatuksella. Sinne on määritetty Yrityksen sisäverkon ip- osoitteet. Kaikki Lead Deskillä tehdyt puhelut nauhoitetaan ja nauhoitteet säilytetään 3 kuukauden ajan koulutusta ja mahdollisia tarkistuksia ja reklamaatioita varten. Nauhoitettuja puheluja pääsee kuuntelemaan ainoastaan kyseisen projektin henkilöt. Lead Deskistä saatavia raportteja käytetään yrityksen sisäisesti toiminnan seurantaan. Lisäksi siitä saadaan puhelintilastoja.

Boosterissa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Siinä on lisäksi ip- osoite tunnistus. Boosterista saatavia raportteja käytetään laskutukseen ja tilastolliseen seurantaan.

Käyttäjän poistuessa yrityksen palveluksesta tieto lopettamispäivästä tulee IT-osaston tietoon ja se poistaa käyttäjätunnuksen välittömästi työsuhteen päättymispäivän jälkeen.

6 Järjestelmien ylläpito ja ylläpitotapahtumien seuranta ja valvonta

Järjestelmiä ylläpidetään Yrityksen tietohallinnon henkilöiden toimesta. Poikkeustapauksissa sovelluksien päivittäminen / ylläpito tapahtuu sovelluksen toimittajan toimesta, jolloin tietohallinnon edustaja valvoo päivitystapahtumaa. Kaikki päivitykset tapahtuvat ennalta sovittujen huoltokatkojen aikana. Päivityksistä kirjataan kuvaus ja tärkeimmät muutokset Muutoshallinta pöytäkirjaan. Lisäksi mahdolliset käyttäjille näkyvät muutokset päivitetään sovellusohjeisiin.

6.1 Järjestelmätoimittajien ja yhteistyökumppaneiden käyttöoikeudet

Pääsääntöisesti Yrityksen järjestelmiin ei pääse Yrityksen ulkopuoliset henkilöt. Jos järjestelmätoimittajan tai yhteistyökumppanin pitää päästä päivittämään tai korjaamaan järjestelmää. niin se tapahtuu Yrityksen IT-osaston henkilön valvonnassa.

7 Asiakkaiden tekemä tietojenluovutuskielto ja tietojen tarkastusoikeuden toteutuminen

Valtaosa yrityksen järjestelmiin tulevista henkilötiedoista on Toimittajan toimittamia tai joltain rekisterinpitäjältä hankittu. Tämä tarkoittaa sitä, että Yritys on rekisterinkäsittelijä eikä rekisterinpitäjä. Tällöin luotetaan siihen, että tietojenluovutuskielto on toteutunut jo Toimittajan tai rekisterinpitäjän toimesta.

7.1 Oikeus saada tietoa henkilötietojen käsittelystä

Asiakaskontakti tilanteessa kontaktin kysyessä tietojen lähdettä käyttäjä kertoo projektiin liittyvän tietojen lähteen. Lisäksi käyttäjä vastaanottaa kontaktin ilmoittaman estopyynnön ja välittää sen Toimittajalle ja lisää sen sulkulistaan. Yrityksen sulkulistalla oleviin asiakkaisiin ei enää kontaktoida.

7.2 Oikeus saada pääsy tietoihin

Kontaktin pyytäessä pääsyä tietoihinsa, käyttäjä vastaanottaa tietopyynnön ja välittää sen Toimittajalle Toimittajan ilmoittamalla tavalla tai käyttäjä ohjaa kontaktin Toimittajan sähköisen tietojenpyyntö lomakkeelle kontaktin niin halutessa.

Asiakkaiden antamat ohjeet löytyvät projektikansioista. Ohjeistus kerrotaan ja annetaan uusille työntekijöille perehdyttämiskoulutuksen aikana.

7.3 Oikeus tietojen oikaisemiseen ja tulla unohdetuksi

Koska Yritys on rekisterinkäsittelijä, eikä rekisterinpitäjä, se ohjaa kohteen tietojenoikaisupyynnöt ja pyynnön tulla unohdetuksi rekisterinpitäjän sähköiselle tietojenpyyntölomakkeelle henkilötietojen vahvistamiseksi. Tämä menettely varmistaa asian oikean käsittelyn.

7.4 Tietojen siirto

Yritys ei rekisterinkäsittelijänä voi siirtää henkilön rekisteritietoja rekisterinpitäjän puolesta. Mikäli tällaisia pyyntöjä tulee niin Yritys ohjaa henkilön rekisterinpitäjän sähköiselle tietojenpyyntölomakkeelle henkilötietojen vahvistamiseksi. Tämä menettely varmistaa asian oikean käsittelyn.

7.5 Vastustamisoikeus

Ei ole todennäköistä, että Yritys kohtaa tilanteen, jossa henkilö vastustaa henkilötietojensa käsittelyä. Vastustamisoikeus tarkoittaa, että tietoja ei saa muuttaa tai hävittää tietoja. Näin kuitenkin tapahtuessa Yritys ohjaa henkilön rekisterinpitäjän sähköiselle tietojenpyyntölomakkeelle henkilötietojen vahvistamiseksi. Tämä menettely varmistaa asian oikean käsittelyn.

7.6 Automatisoidut yksittäispäätökset ja profilointi

Yritys ei tee automaattista profilointia, eikä automatisoituja yksittäispäätöksiä.

8 Tehdyt kehittämistoimenpiteet ja havaitut kehittämiskohteet

Omavalvontaa suoritetaan ja kehitetään tietosuojavuosikellon mukaisessa rytmissä. Yrityksellä on tarkoitus kuluvan kalenterivuoden aikana saada aikaan tarkempi omavalvontasuunnitelma. Tiedostojen siirrossa on huomattu kehittämisen tarpeita ja siihen on tilattu latauspalvelu, joka on HTTPS suojattu verkkosivu. Tänne Toimittaja voi siirtää kampanjan tiedot tietoturvallisesti. Tälle alueelle pääse ainoastaan tunnistautumalla käyttäjätunnus – salasana parilla.

8.1 Kehittämiskohteiden seuranta

Yrityksen käyttämän tietosuojavuosikellon avulla seurataan säännöllisesti kehittämiskohteiden tilaa. Lisäksi omavalvonnan kehitystä seurataan Yrityksen johdon toimesta.