Euroopan laajuista tiedonhallintaa

EU:n yleinen tietosuoja-asetus (GDPR = General Data Protection Regulation) perustuu EU:n laajuiseen yhteiseen tiedonhallintaan. GDPR:n tarkoituksena on yhdenmukainen henkilötietojen käsittelysäännöstö EU:n alueella ja tämän edellytyksenä on taas yhdenmukaiset termit ja käsitteet, jotka luovat alueelle yhteisen henkilötietoja koskevan kielen. Asetus määrittelee myös, miten ja milloin henkilöitä on informoitava heidän henkilötietojensa käsittelystä. Kaiken kaikkiaan tämä on valtava haaste ja näin ollen on ymmärrettävää, että GDPR:n toteutusta valvotaan ja puutteet on sanktioitu. Seuraavassa kuvaan toteutukseen liittyviä ongelmia sekä myös mahdollisuuksia.

Mitä kuuluu GDPR?

EU:n yleinen tietosuoja-asetus (GDPR = General Data Protection Regulation) on täysimääräisesti ollut voimassa yli kaksi vuotta, sillä sen siirtymäkausi päättyi 25.5.2018. Suomen oma täydentävä Tietosuojalaki HE 9/2018 tuli voimaan 1.1.2019 ja tällöin kumoutui vanha Henkilötietolaki. Tietosuojavaltuutetun toimisto on organisoitunut valvomaan tietosuojalainsäädännön noudattamista. Toimistossa on tietosuojavaltuutettu ja kaksi apulaistietosuojavaltuutettua, jotka yhdessä muodostavat seuraamusmaksuista päättävän seuraamuskollegion. Lisäksi toimistossa on n. 40 asiantuntijaa.

Aluksi pari esimerkkiä Tietosuovaltuutetun toimistossa tehdyistä päätöksistä.

1.Ovenavaustiedot ovat henkilötietoja.

Taloyhtiössä on käytössä asuinrakennuksen ulko-oviin asennettu sähkölukitusjärjestelmä. Taloyhtiössä oli arvioitu, ettei sähkölukkojärjestelmän käyttöön ja ovenavaustietojen tallentamiseen liity henkilötietojen käsittelyä. Mutta sähköavainten käyttäjät voidaan kuitenkin tunnistaa, kun yhdistetään avaimen yksilöinti tieto tiettyyn asuntoon. Erityisesti yksinasuvien henkilöiden kohdalla ovenavaustiedot voidaan yhdistää tiettyyn henkilöön. Näin ollen ovenavaustiedot muodostavat henkilörekisterin.

Henkilötietojen käsittely edellyttää aina käsittelyperustetta ja tietosuojasääntelyn noudattamista. Asunto-osakeyhtiö ei ollut arvoinut tiedonkeruun tarpeellisuutta eikä tietojen säilytysajan rajoittamista. Yhtiö ei ollut myöskään informoinut asukkaille läpinäkyvästi henkilötietojen käsittelystä, joten sen suorittama henkilötietojen käsittely on laitonta. Apulaistietosuojavaltuutettu määräsi yhtiön muuttamaan henkilötietojen käsittelyn tietosuoja-asetuksen mukaiseksi. Lähde: Tietosuovaltuutetun toimiston tiedote 3.8.2020

2. Ääntä ja kuvaa tallentava kameravalvontajärjestelmä taksissa.

Taksi Helsinki uusi kameravalvontajärjestelmänsä, mutta ei huomannut arvioida siihen liittyvien henkilötietojen lainmukaisuutta. Tämän seurauksena Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi Taksi Helsingille 72 000 euron suuruisen seuraamusmaksun.

Mitä Taksi Helsinki laiminlöi? Tietosuovaltuutetun toimiston tiedotteessa 29.5.2020 on Taksi Helsingin tapausta käsitelty seikkaperäisesti ja avattu apulaistietosuojavaltuutetun selvitystä:

1) Henkilötietojen käsittelystä ei kerrottu tietosuojalainsäädännön edellyttämällä tavalla asiakkaille. Takseissa olevissa ilmoituksissa ei kerrottu äänen tallentamisesta eikä siitä mistä asiakkaat olisivat voineet saada tiedon.
2) Yhtiö ei kertonut kanta-asiakasohjelmaan liittyvästä automaattisesta päätöksenteosta ja siihen liittyvästä profiloinnista tietosuojaselosteessaan.
3) Dokumentoinnissa ja henkilötietojen käsittelyyn liittyvissä rooleissa oli puutteita.

Selvityksessä ilmeni vakavia puutteita riskien tunnistamisessa, tietosuojaperiaatteiden sekä rekisteröidyn oikeuksien noudattamisessa, ja siksi seuraamuskollegio määräsi Taksi Helsingille seuraamusmaksun. Lähde: Tietosuovaltuutetun toimiston tiedote 29.5.2020.

Henkilörekisterin tunnistus

Nämä esimerkit osoittavat kuinka tärkeätä on ottaa tietosuoja osaksi suunnitteluprosessia aivan alusta alkaen. Kaikkein ensimmäiseksi on tarkoin arvioitava, muodostaako tulevan ratkaisun jokin osa henkilörekisterin.

Tavanomaiset henkilötiedot ovat: etunimi, sukunimi, syntymäaika, henkilötunnus, osoite, puhelinnumero, sähköpostiosoite, kuvat, videot, äänitteet, sijaintitiedot ja muut tiedot, joista henkilö voidaan tunnistaa välillisesti tai välittömästi. Sensitiivisiä, erityisiä henkilötietoja ovat: etninen tausta, seksuaalinen suuntaus, poliittinen suuntaus, uskonto, ammattiyhdistyksen tai –liiton jäsenyys, terveystiedot, geneettinen data, biometrinen data (esim. sormenjäljet, iirisskannaus), rikosrekisteri tai muut rikkomuksiin liittyvät tiedot. Tyypillisiä henkilörekistereitä ovat: asiakas-, markkinointi-, henkilöstö-, yhteistyökumppani- ja jäsenrekisterit. Rekisteri voi olla myös perinteisessä paperimuodossa mapissa.

Käyttötarkoitus ja roolit

Henkilörekisterin tunnistuksen lisäksi on tarkoin harkittava ja määriteltävä henkilötietojen käyttötarkoitus sekä henkilötiedon koko elinkaari. Tietoja saa tallentaa rekisterissä ainoastaan käyttötarkoituksen vaatiman ajan, ei yhtään sen pidempään. Erityisesti näihin seikkoihin on tietosuojavaltuutetun toimistossa puututtu ja annettu huomautuksia ja seuraamusmaksuja.

Henkilötietojen käsittelyn tarkoitus pitää yksilöidä, dokumentoida sekä kertoa rekisteröidylle helposti ymmärrettävässä muodossa niin, että tieto on vaivattomasti rekisteröidyn saatavissa. Tarkoituksena on luoda ja ylläpitää rekisterinpitäjän ja rekisteröidyn välistä luottamusta. Tässä luottamuksessa piilee koko GDPR:n ”juju”, jota kannattaa hyödyntää. Hyvä luottamussuhde on kilpailuetu.

Käyttötarkoituksen tarkka määrittely ja dokumentointi auttaa rekisteröityä ymmärtämään, mihin hänen tietojaan käytetään ja miettimään haluaako hän käyttää tietosuojaoikeuksiaan, jotka ovat:

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.

Henkilötietojen rekisteröintiin kuuluvat roolit tulee selventää ja dokumentoida. Roolit **rekisterinpitäjä** (controller) ja **käsittelijä** (processor) ovat osoittautuneet hankaliksi ymmärtää oikein ei vain Suomessa vaan myös Euroopan laajuisesti. Ne ovat kuitenkin aivan oleellisia GDPR:n näkökulmasta, koska ne ovat asetuksen termejä. Esimerkiksi asetuksen luvussa 4 artiklassa 24 käsitellään rekisterinpitäjän vastuuta ja artiklassa 28 henkilötietojen käsittelijän tehtäviä ja velvoitteita sekä myös rajoituksia. On selvää, että jos peruskäsitteet ovat sekaisin niin sotkuhan siitä seuraa. Toisin sanoen noissa artikloista ei saa tolkkua. Erityisesti roolin controller suomentaminen sanaksi rekisterinpitäjä on aiheuttanut kritiikkiä ja myös käytännön sekaannusta. Tietosuojavaltuutetun toimisto on mm. julkaissut tiedotteen 5.8.2019 ”Henkilötietojen käsittely yhdistystoiminnassa”, jossa hyvin selkeästi käydään läpi urheiluseurojen ja muiden yhdistysten osalta terminologiaa sekä vastuita paikallisyhdistyksen ja katto-organisaation välillä.

Tietosuovaltuutetun toimiston sivuilla (tietosuoja.fi) on hyvä, kattava ohjeisto, jota kannattaa seurata. Sieltä selviää myös mahdolliset muutokset, joita ajan myötä tietosuoja-asioihin tulee. Seloste käsittelytoiminnasta ja rekisteröidyn informointi velvoite on kuvattu taulukon muodossa. Ne on hyödyllistä ottaa käyttöön heti kehitystyön alussa ja pitää koko projektin ajan rinnalla muistuttamassa GDPR:n asettamista vaateista. Taulukot ovat Rekisterinpitäjän seloste käsittelytoimista, Henkilötietojen käsittelijän seloste käsittelytoimista ja Informointivelvoitteen edellyttämät tiedot (pdf).

GDPR kilpailuetuna

GDPR on laadittu vahvistamaan yksilön oikeuksia. Sen noudattaminen kannattaa nähdä osana yrityksen imagoa sekä kilpailutekijänä. Nykytilanteessa useimmat organisaatiot ovat toteuttaneet GDPR:n vaatiman informoinnin päivittämällä tietosuojaselosteen, joka avautuu organisaation www-sivujen alareunassa. Vaatimukset ja niiden toteutus voidaan ottaa osaksi palvelumuotoilua, jonka keskeisenä tavoitteena on luoda hyvä asiakaskokemus. Tässä yhteydessä analysoidaan kaikki ne tilanteet, missä asiakas kohtaa henkilötietojaan ja varmistetaan, että hän saa jokaisessa kohdassa tarvittavat tiedot henkilötietojensa käsittelystä. Kun vielä ilmaistaan asiat asiakkaalle ja yrityksen imagolle sopivalla kielellä, niin vaatimuksista syntyykin asiakkaan ja yrityksen välistä luottamusta vahvistava tekijä.

Hyödyllisiä tietolähteitä

Tietosuoja.fi
Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.
Tietosuojalaki HE 9/2018
Tietosuoja käsikirja johdolle, Ari Andreasson; Juha Koivisto; Arto Ylipartanen
Osaava tietosuojavastaava, Ari Andreasson; Jaana Riikonen; Arto Ylipartanen
Työpaikan tietoturvaopas, Petteri Järvinen & Kimmo Rousku
Tekoäly matkaopas johtajille, Antti Merilehto
Selviytymisopas EU:n tietosuoja-asetuksen pykäläviidakkoon, Paula Miinalainen
Kuntaliiton Yleiskirje 14/2017 Kunnan- ja kaupunginhallituksille, kuntayhtymien hallituksille
Tietosuojavaltuutetun toimiston tiedote 5.8.2019 ohje ”Henkilötietojen käsittely yhdistystoiminnassa”