GDPR – The Final Countdown

- **Työttömäksi puolessa vuodessa – tietosuoja-asiantuntijan tavoite ennen toukokuuta 2018**
  Laura Tarhonen, Sanoma
- **Puretaan myyttejä – GDPR ja suostumus**
  Pia Pynnä, ASML
- **11 GDPR-vinkkiä markkinoijalle**
  Ben Ottoman, Avaus Marketing Innovations

Työttömäksi puolessa vuodessa – tietosuoja-asiantuntijan tavoite ennen toukokuuta 2018

Datan merkitys kasvaa, digitaalisuus on oletus ja jokainen omistamamme laite on yhteydessä verkkoon. Henkilötiedon määritelmä on niin laaja, että edellä mainituilla ilmiöillä on selkeä yhteys myös tietosuojan merkitykseen. Tietosuojasta tulee väistämättä yksi niistä tavanomaisista osaamisalueista, joita edellytetään jokaiselta, joka millään tavalla käsittelee tai sivuaa henkilötietoja työssään. Fiksut rekisterinpitäjät ajavat jo nyt – tai viimeistään kohta – asennemuutosta, jossa tietosuojasta tehdään osa jokaisen työntekijän vastuita. Olen kutsunut tätä muutosta leikkimielisesti *tietosuojavallankumoukseksi*. Se on vallankumous, jossa tietosuoja-asiantuntijat ovat etulinjassa, vaikka sen tarkoitus on tehdä juuri heistä itsestään tarpeettomia levittämällä osaamista laajemmalle joukolle organisaatiossa.

Tietosuoja-asetus tulee edellyttämään sisäänrakennettua ja oletusarvoista tietosuojaa. Vaatimus ei ole täysin uusi. Jo tälläkin hetkellä henkilötietojen käsittelyn tulee olla huolellista, etukäteen suunniteltua ja sidottua tiettyihin käyttötarkoituksiin. Asetus kuitenkin edellyttää, että rekisterinpitäjät pystyvät osoittamaan, kuinka vaatimukset on toteutettu henkilötietojen käsittelyssä. Käytännössä vaatimustenmukaisuus on pystyttävä todistamaan dokumentaatiolla, joka voi esimerkiksi sisältää tietosuojavaikutusarviointien tuloksia, prosessikuvauksia ja ohjeistuksia.

Mitä sisäänrakennettu tietosuoja sitten tarkoittaa tietosuoja-asiantuntijan näkökulmasta? Se laajentaa tietosuojaosaamisen tarpeen henkilöstön läpileikkaavaksi ja painottaa koulutuksen, työkalujen ja prosessien merkitystä tietosuoja-asiantuntijan työssä. Enää ei riitä, että lakiosastolla kirjoitetaan rekisteriseloste ja käyttöehdot, ja julkaistaan ne verkkosivustolla. Vastuu tietosuojavaatimusten toteuttamisesta tulee olla siellä, missä datan keräämiseen ja käsittelyyn liittyviä päätöksiä tehdään. Myös tietoisuus erilaisten valintojen vaikutuksista on ujutettava arkipäiväisiä päätöksiä tekeville tahoille, kuten esimerkiksi markkinointi-, digikehitys- tai HR-tiimeille.

Koulutusta ja tietoisuutta

Ensimmäinen, ja ehkä tärkein, askel tietosuoja-asiantuntijan tarpeettomaksi tekemisessä on koulutuksen ja tietoisuuden lisääminen. Tämä voi tuntua mahdottomalta ja massiiviselta tehtävältä, kun rekisterinpitäjän palveluksessa on usein maksimissaan muutama tietosuoja-asiantuntija ja satoja, ellei tuhansia muita työntekijöitä. Jos tehtävä on liian suuri, kannattaa se paloitella ja laittaa palat tärkeysjärjestykseen. Tämä on hyvä periaate myös koulutusten osalta. Erilaisissa rooleissa olevat työntekijät tarvitsevat eriasteista tietosuojatietoisuutta. Suurelle osalle organisaatiota voi riittää se, että suoritetaan esimerkiksi verkkokurssi tietosuojan perusteista ja rekisterinpitäjän tietosuojapolitiikasta. Verkkokurssin vaikuttavuutta voi tehostaa järjestämällä lyhyitä tietoiskuja tai muita kaikille avoimia tapahtumia, joissa tietosuojaperiaatteita selostetaan yleisellä tasolla.

Niin yleisissä kuin kohdennetummissakin koulutuksissa on hyvä aloittaa vetoamalla osallistujien omaan arvomaailmaan ja määritelmään yksityisyydestä. Usein tietosuojasta tulee konkreettista vasta kun siihen kohdistuvan loukkauksen pystyy

demonstroimaan hyvällä esimerkillä. Tyypillisesti, tietovuodoista tai muista ylilyönneistä tehdyt uutisjutut toimivat hyvin. Myös analogia fyysisestä yksityisyydestä digitaaliseen yksityisyyteen voi olla silmiä avaava. Ihmiset eivät ole välttämättä tulleet ajatelleeksi, miten yksityisyys fyysisessä maailmassa (esimerkiksi kotirauha) on heille täysin itsestään selvää, mutta heillä ei ole minkäänlaista käsitystä digitaalisesta yksityisyydestään.

Yleisten koulutusten lisäksi tulisi tunnistaa kaikki ne ryhmät, jotka ovat avainasemassa tietojen keräämisessä tai muussa käsittelyssä. Riippuen rekisterinpitäjästä, tällaisia ryhmiä löytyy ainakin tuotekehityksen, raportoinnin, myynnin, markkinoinnin, analytiikan ja HR:n parista. Kaikille tällaisille ryhmille tulisi järjestää kohdennettua tietosuojakoulutusta. Parhaimmat tulokset syntyvät tyypillisesti jos koulutuksen sisältöä voidaan räätälöidä sen perusteella, minkälaisia tietosuojakysymyksiä kyseiset henkilöt kohtaavat työssään. Onkin hyvä jututtaa yhtä tai muutamaa osallistujista etukäteen ja kartoittaa minkälaisia teemoja koulutukseen tulisi sisällyttää. Sääntöjen läpikäynti konkreettisten tapausten pohjalta antaa mahdollisuuden vuorovaikutukseen osallistujien kanssa ja samalla materiaalista tulee suora ohjenuora, jota voi hyödyntää käytännön työssä. Usein koulutusten aikana voidaan myös yhdessä tunnistaa minkälaisia standardoituja ohjeistuksia tai vaikkapa sopimuspohjia kyseessä olevalle alueelle voitaisiin tarvita.

Koulutusten kautta kasvavan tietoisuuden myötä tietosuoja-asiantuntijoiden on hyvä valmistautua myös kysymysten ja avun tarpeen kasvamiseen. Pelkkä tietoisuus ei riitä, koska teot ratkaisevat. Rekisterinpitäjän on tarjottava mahdollisuus myös noudattaa tietosuojavaatimuksia; muuten vallankumous jää puolitiehen. Syntynyttä innostusta ja kiinnostusta on ruokittava selkeillä ohjeilla ja prosesseilla. Jos konkreettisia toimenpiteitä ei mahdollisteta, ihmiset väistämättä ajattelevat, ettei asia olekaan niin tärkeä.

Työkaluja ja prosesseja

Vaatimuksina erityisesti sisäänrakennettu ja oletusarvoinen tietosuoja tukevat ajatusta siitä, että rekisterinpitäjien kannattaa satsata vaikutustenarviointi-prosessin rakentamiseen, vaikkei käsittely edellyttäisikään asetuksen 35 artiklan mukaista arviointia. Arvioimalla tietosuojavaikutuksia esimerkiksi osana tuotekehitysprosessia, rekisterinpitäjä voi paitsi varmistaa, että tietosuojavaatimukset ja sisäänrakennettu tietosuoja otetaan huomioon, myös dokumentoida kehitykseen mahdollisesti liittyvät riskit ja toimenpiteet riskien lieventämiseksi. Kuulostaa kuitenkin helpommin sanotulta kuin tehdyltä ja näin se usein onkin. Standardoituun tuotekehitysprosessiin voi olla helppoa lisätä normaalin teknisen dokumentaation lisäksi tietosuoja ja -turva-arvioinnit. Vaikutustenarvioinnille voi kuitenkin olla hankalampaa löytää sopivaa paikka, jos käynnissä ei ole kehitystä tai muuta määriteltyä prosessia, esimerkiksi markkinointikampanjoita saatetaan tehdä tarpeen mukaan lyhyelläkin varoitusajalla. Hyvänä nyrkkisääntönä voi käyttää sitä, että täysin uuteen datan käsittelyyn tehdään aina uusi arviointi ja että "vanhaan" tai usein toistuvaan käsittelyyn tehdään ohje. Uusi arviointi tehdään vain jos käsittelyyn halutaan tehdä muutoksia tai ohjeita ei pystytä sellaisenaan noudattamaan.

Vapaamuotoiset tietosuojaa koskevat vaikutustenarvioinnit (eivät perustu suoraan artiklaan 35) voivat olla varsin monenmuotoisia. Usein voikin olla tarpeellista kehittää muutama rinnakkainen arviointiprosessi, joita hyödynnetään tilanteesta riippuen. Tuotekehitykseen voidaan laatia tietosuojavaatimusten listaus, jonka toteuttaminen varmistetaan dokumentoimalla vaikutustenarviointi. Samalla prosessilla voidaan myös tehdä vaikutustenarviointeja sellaisistakin tuotteista, jotka ovat jo

markkinoilla. Tällöin vaikutuksia arvioidaan jälkikäteen, eikä kuten tietosuoja-asetus edellyttää, eli ennen käsittelyn aloittamista. Fakta kuitenkin on, että jostain on aloitettava ja kuten sanonta kuuluu: parempi myöhään kuin ei milloinkaan.

Markkinointiin ja muihin tiedon hyödyntämiseen liittyviin käyttötapauksiin voidaan tehdä oma vaatimuslistansa ja vaikutusarviointinsa. Näissä keskitytään kehitysvaatimusten (esimerkiksi: "näin kysytään markkinointilupaa") sijaan tietoon liittyviin käyttörajoituksiin, käsittelyn perustan ja läpinäkyvyyden varmistamiseen sekä vaikutuksiin loppukäyttäjälle. Kannattaa myös pohtia, halutaanko tehdä teknisiä järjestelmiä koskevia vaatimuksia ja niihin liittyviä vaikutusarviointeja tai arvioida tietojen käsittelyä prosessinäkökulmasta. Esimerkiksi työntekijöiden henkilötietojen käsittely liittyy tyypillisesti johonkin yrityksen prosessiin, kuten rekrytointiin. Rekrytointiprosessin henkilötietojen käsittelyä voikin olla viisainta arvioida prosessinäkökulmasta ennemmin kuin esimerkiksi järjestelmänäkökulmasta.

Vaikutustenarviointien dokumentoiminen voi olla raastavaa. Kun tietosuoja-asiantuntija totaalisesti kyllästyy excel- ja word -dokumenttien päivittelyyn ja versionhallintaan, voi hän harkita teknisen työkalun hankintaa. Tietosuoja-asetus on luonut valtavan kysynnän työkaluille, joihin vaikutustenarviointeja voidaan dokumentoida. Markkinoilla on kymmeniä erilaisia työkaluja, joista oleellista on valita omalle organisaatiolle oikea. Kannattaa myös muistaa, että vaikka kuinka hieno työkalu on, se ei itsenäisesti tee arviointeja, vaan tietosuoja-asiantuntijan on koulutettava keskeiset tahot näpyttelemään vastauksia työkaluun.

Kun vaikutusarviointiprosessit on määritelty, vaatimukset on dokumentoitu, mahdollinen työkalu on hankittu ja käyttövalmis, tietosuoja-asiantuntijan tulee enää jalkauttaa prosessi organisaatioon. Tässä vaiheessa joutuu usein palaamaan koulutuksiin ja tietoisuuden lisäämiseen.

Ohjeistukset ja standardoidut vastaukset

Hyvä tietosuoja-asiantuntija on sisäsyntyisesti laiska. Jos samaa asiaa kysytään useamman kerran, asiantuntijan vastauksesta luodaan ohje ja ohje levitetään relevanteille tahoille. Jos mahdollista, ohjeen sisältö opetetaan tyhjentävästi yhdelle kysyjälle, jonka jälkeen muut ohjataan tämän "tietosuojaoppineen" luokse. Tämän jälkeen tietosuoja-asiantuntijalle tulee samasta asiasta kysymyksiä vain, jos 1) ohjeen olemassaolo on unohtunut tai ei ole tiedossa, 2) halutaan toimia ohjeen vastaisesti tai 3) kyseinen tapaus ei ole täysin vastaava kuin ohjeessa. Näistä vain kohdat 2 ja 3 edellyttävät lisätyötä, jonka voi kuitenkin suoraan lisätä ohjeeseen, jotta se on tulevaisuudessa kattavampi. Tämäkin saattaa kuulostaa liian hyvältä ollakseen totta ja näin se usein on. Tällaiseen toimintatapaan on kuitenkin pyrittävä. Muuten tietosuoja-asiantuntija ei itsekään voi olla varma vastaavansa samanlaisiin kysymyksiin aina samalla tavalla. Keskitettyjä ohjeita tehtäessä dokumentaatio pysyy selkeänä, sen sijaan että vastattaisiin aina ad hoc -kysymyksiin erikseen.

Tietosuoja-asiantuntijan lisäarvo organisaatiolle syntyy hänen kyvystään tunnistaa, minkälaisista asioista voidaan tehdä standardoituja ohjeita ja tuottaa ne. Ohjeiden ei tarvitse olla mustavalkoisia ("näin saa, tai ei saa tehdä"). Ne voivat olla tyylitään sellaisia, joissa annetaan erilaisia vaihtoehtoja ja joista voidaan valita, riippuen siitä minkälaisia sisäänrakennettua ja oletusarvoista tietosuojaa toteuttavia toimenpiteitä voidaan ottaa huomioon ja toteuttaa. Järkevästi standardoimalla erilaisiin aihealueisiin liittyviä tyypillisiä kysymyksiä, tietosuoja-asiantuntija vapauttaa oman aikansa kaikkein

haastavimpiin kysymyksiin sekä edellä esitettyjen osa-alueiden (koulutusten ja vaikutustenarviointien) kehittämiseen.

Kaiken tämän jälkeen - jääkö tietosuoja-asiantuntija seisomaan vallankumouksen raunioihin työttömänä? Ei jää. Kuin feeniks tuhkasta nousten, tietosuoja-asiantuntija jatkaa tietosuojavastaavana. Tietosuojavastaavana hänen roolinsa on kuitenkin hieman erilainen, sillä siinä on vahvemmin mukana vaatimuksenmukaisuutta valvova elementti. Kuvainnollisesti, kun auto on saatu koottua ja sen ajolle on määritelty liikennesäännöt, siirrytään valvomaan ajetaanko liikennesääntöjen mukaisesti ja raportoidaan rikkeistä. Jotta liikennesäännöt eivät unohdu, niitä on syytä edelleen säännöllisesti opettaa ja aina uuden tilanteen vastaan tullessa tulee määritellä uusia sääntöjä.

Laura Tarhonen (OTM, CIPP/E)
Privacy Manager
Sanoma

Puretaan myyttejä – GDPR ja suostumus

Tietosuoja-asetuksen eli GDPR:n suostumuksesta liikkuu valtava määrä "totuuksia" ja kaupunkihuhuja. Kuten että jatkossa kaikki henkilötietojen käsittely, profilointi ja b2b sähköinen suoramarkkinointi mukaan lukien edellyttäisi nimenomaista suostumusta. Tai että kaikki vanhat suostumukset on uusittava. Mikä on totta ja mikä kaupunkihuhuja?

1. Suostumus nyt ja jatkossa – tuleeko kaikkeen käsittelyyn saada suostumus?

Vastaus on yksiselitteisesti ei. Tällä hetkellä Suomessa henkilötietolaki säätää yleisistä edellytyksistä, joiden perusteella henkilötietoja voidaan käsitellä. Samalla tavalla tietosuoja-asetuksessa määritetään kuusi perustetta henkilötietojen käsittelylle. Ja ihan niin kuin henkilötietolaissa, tietosuoja-asetuksessakin suostumus on vain yksi käsittelyperuste muiden joukossa.

Suostumusta käsittelyperusteena miettiessä huomioon kannattaa ottaa myös se, että suostumus antaa joissain tapauksissa vahvempia oikeuksia, kuten oikeuden tulla unohdetuksi ja oikeuden tietojen siirtoon, kuin silloin jos käsittelyperusteena olisi vaikka oikeutettu etu.

2. Erota viestien lähettäminen yleisestä käsittelystä

Suostumusta koskevia pohdintoja tehtäessä tulee heti kättelyssä erottaa toisistaan suostumus yleisesti henkilötietojen käsittelyyn ja suostumus (sähköisten) viestien lähettämiseen. Nämä ovat eri asioita ja niitä koskee myös osittain eri lainsäädäntö.

Tietosuoja-asetus ei sääntele kanavakohtaisista luvista, vaan nämä tulevat jatkossa valmisteilla olevasta ePrivacy -asetuksesta (Suomessa tällä hetkellä tietoyhteiskuntakaaressa), jonka oli alun perin tarkoitus tulla voimaan samanaikaisesti GDPR:n kanssa, mutta jonka valmistelu on takunnut niin, että on aivan varmaa, ettei näin käy. Evästeiden ja b2c sähköisen suoramarkkinoinnin lisäksi myös mm telemarkkinointi ja b2b sähköpostimarkkinointi ovat käsittelyssä tässä putkessa.

3. Suostumuksen määritelmä nyt ja jatkossa – mikä muuttuu?

Usein kuulee, että tietosuoja-asetuksen suostumus tarkoittaa nimenomaista suostumusta eikä nykyisen kaltaista yksiselitteistä suostumusta. Onko näin ja mitä ihmettä tämä edes tarkoittaa?

Tietosuoja-asetuksesta ei ole tulossa nimenomaisen suostumuksen vaatimusta kaikelle käsittelylle (jossa suostumusta pyydetään), vaan se koskee nykyisen lainsäädännön tavoin vain tiettyjä käsittelyjä kuten esimerkiksi arkaluonteisia tietoja tai automatisoituja päätöksiä. Asetuksessa ei löydy määritelmää nimenomaiselle suostumukselle. Näyttää kuitenkin siltä, ettei se juurikaan eroa tavanomaisesta yksiselitteisestä suostumuksesta paitsi sen osalta, että nimenomainen suostumus tulee vahvistaa selkeällä kirjallisella tai suullisella lausumalla, joka viittaa johonkin tiettyyn nimenomaiseen käsittelyyn, kun yksiselitteiseen suostumukseen riittää epäsuora myöntyminen eli käytännössä:

Epäsuora/yksiselitteinen suostumus:
Anna sähköpostiosoitteesi (vapaaehtoinen)
"Käytämme osoitettasi lähettääksemme tarjouksia ja tietoa tuotteistamme"

Nimenomainen suostumus:
"Suostun vastaanottamaan sähköpostia tuotteistanne ja saaman tarjouksia siivousvälineistä (rasti ruutuun)"

4. Tarkemmat raamit

Nopeasti katsottuna näyttää siis jokseenkin samankaltaiselta tilanne nyt ja jatkossa. Mutta kun luetaan asetusta eteenpäin, löytyy erojakin.

Tietosuoja-asetuksessa (art 7) asetetaan neljä edellytystä, jotka suostumuksen on täytettävä:

- On pystyttävä osoittamaan, että suostumus on annettu
- On annettava mahdollisuus suostumuksen peruuttamiseen ja kerrottava siitä
- On esitettävä pyyntö selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa, selkeällä ja yksinkertaisella kielellä
- Eikä palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi voi asettaa suostumusta sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten

Miten nämä suhtautuvat nykylainsäädäntöön – muuttuuko todellisuudessa kuitenkaan niin paljoa? Alla käsitellään näitä neljää edellytystä hieman tarkemmin.

4.1. Suostumus pitää näyttää toteen

Nykylainsäädännössä asiaan ei ole varsinaisesti otettu kantaa, mutta käytännössä tilanne ei silti muutu, sillä jo henkilötietolain perusteluissa on todettu, että suostumuksen pyytäjän tulee näyttää toteen suostumuksen olemassaolo. Jatkossa suostumuksesta olisi kuitenkin hyvä jäädä tarkemmin tieto siitä kuka suostui, mihin suostui, milloin ja millä tavoin suostui, mitä informoitiin suostumuksesta ja onko suostumus peruutettu.

4.2. Suostumuksen peruuttaminen ja siitä kertominen

Jo tällä hetkellä henkilötietolain perusteluissa todetaan, että rekisteröidyllä on oikeus milloin tahansa peruuttaa suostumuksensa. Vain peruutusoikeudesta kertominen tulee siis teoriassa uutena, mutta käytännössä tämäkin on sisältynyt yleiseen informointivelvollisuuteen. Jatkossa kannattaa tämänkin osalta varmistaa, että peruutusoikeudesta on kerrottu selkeästi muun informaation ohessa.

4.3. Suostumuksen pyytämisen tapa – nykyiset luvat romukoppaan?

Todella usein eri tilaisuuksissa ja yhteyksissä on viimeisen vuoden aikana kuullut väitteen, että asetuksen tullessa voimaan nykyiset suostumukset muuttuvat pätemättömiksi ja tämän vuoksi nyt tulisi alkaa keräämään kiireen vilkkaan uusi lupia.

Näin suoraviivaista ja mustavalkoista asia ei kuitenkaan ole. Ja täysin varmaa on se, ettei uusia lupia tarvitse kerätä, mikäli nykyiset on kerätty asetuksen vaatimukset täyttäen. Tämä on todettu jo asetuksen resitaaleissa (171). Mitä nämä vaatimukset sitten ovat?

Asetuksessa edellytetään, että suostumusta pyydettäessä kerrotaan vähintään se, kenelle suostumus pyydetään, mihin tarkoituksiin ja miten käsitellään sekä peruutusoikeus. Asetuksen resitaalien mukaan **" ....Suostumusta ei sen vuoksi pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta..."**

Kannattaa myös huomioida se, ettei asetuksen edellyttämä "aktiivinen toimi" suinkaan sulje pois nykyistä epäsuoraa suostumusta edellyttäen, että siihen liittyy jonkinlainen toimi, joka osoittaa selkeästi suostumuksen tietojen käsittelyyn tietyllä tavalla. Myöskään jatkossa "rasti ruutuun" ei tule olemaan ainoa tapa suostumuksen pyytämisen.

Muita ihan yhtä hyviä tapoja on esimerkiksi kirjallisen dokumentin allekirjoittaminen, "opt-in" näppäimen tai linkin painaminen, kyllä/ei valinnan tekeminen, valintojen tekeminen asetuspaneelissa, vastaaminen sähköpostiin jossa pyydetään suostumusta, myöntävä vastaus suulliseen luvankysymiseen tai vapaaehtoisten tietojen antaminen tiettyyn tarkoitukseen. Se mitä ei kannata tehdä, nyt tai jatkossa, on nojautua passiivisuuteen, valmiiksi rastitettuihin ruutuihin, "opt-out" ruutuihin, oletusasetuksiin tai ehtoihin piilotettuun suostumukseen.

Jos kuitenkin vuosien varrella on tullut kerättyä lupia, joiden alkuperästä ei ole täyttä varmuutta, kannattaa miettiä keinoja lupien tuoreuttamiseen (esimerkiksi hyvällä informaatiolla) tai muita perusteita käsittelyn jatkamiselle.

4.4. Käsittely palvelun edellytyksenä – saako?

Aika yleinen käytäntö nykyään on, että suostumus on asetettu palvelun käyttämisen edellytykseksi. Jatkossa ongelmia voi tämän osalta aiheuttaa se, että tietosuoja-asetus on selkeä sen suhteen, ettei suostumusta voi bundlata palvelun ehdoksi, ellei se ole välttämätön palvelun toimimiseksi.

Jos kuitenkin päädytään suostumukseen, kannattaa ottaa huomioon se, että käytännössä se, onko suostumus "tarpeellinen sopimuksen täytäntöön panemiseksi" tarkoittaa esimerkiksi sitä, että verkkokaupan asiakkaiden tietojen jakaminen muiden verkkokauppojen kanssa ei välttämättä täytä tätä edellytystä, mutta tietojen jakaminen rahdinkuljettajan kanssa sitä vastoin täyttää. Näin ollen ensimmäisessä tapauksessa voi olla, ettei suostumusta katsota annetun "vapaasti", mutta toisessa suostumus on ilman muuta "vapaasti" annettu.

UK:n tietosuojavaltuutettu on kuitenkin todennut, että joissain rajoitetuissa tapauksissa sopimuksen edellytyksenä ollut suostumus voitaisiin katsoa annetun "vapaasti", vaikka käsittely ei olisikaan tarpeellista sopimuksen täytäntöön panemiseksi. Tällaisia olisi esimerkiksi se, ettei suostumukselle ole vaihtoehtoa, käsittely lopetetaan, jos suostumus peruutetaan, informointi on selkeää ja suostumuksen bundlaaminen palveluun on kohtuullista. Näitä soveltaen tilanne ei enää niin kovin erilaiselta näytäkään, mutta pohdittavaksi tulee vielä se, mitä tapahtuu, jos suostumus peruutetaan – loppuuko palvelu, jatkuuko "huonompana" vai sellaisenaan? Kaksi ensimmäistä vaihtoehtoa johtava jälleen kysymykseen siitä, onko suostumus annettu "vapaasti".

5. Profilointi edellyttää aina suostumusta

Asetuksessa ei edellytetä profiloinnin käsittelyperusteeksi suostumusta, vaan se kuuluu edelleen moneen toimintaan GDPR:n sallimana peruselementtinä ja voisikin sanoa, että käsittelyperusteen löytyessä, oli se mikä tahansa, profilointi on lähtökohtaisesti sallittu. Jokunen mutka tähänkin tulkintaan kuitenkin saadaan.

Vuoden 2017 loppupuolella EU:n tietosuojaviranomaisten työryhmä WP29 julkaisi nimittäin ohjeistusluonnoksen, jonka mukaan asetuksen artikla 22(1) olisi kielto tehdä automaattista päätöksentekoa, joka sisältää profilointia, ellei sovellettavaksi tulisi poikkeuksia kuten nimenomainen suostumus tai sopimuksen täytäntöönpano (jota tulkitaan ohjeen mukaan erittäin suppeasti). Ja sanoopa selkeästi alaviitteessä, ettei rekisterinpitäjän oikeutettu intressi ole artiklan 22(1) tapauksessa laillinen käsittelyperuste.

Tulkinta tarkoittaa käytännössä sitä, että jos esimerkiksi online-mainonnan taustalla oleva tietojenkäsittelyn tulkitaan aiheuttavan "oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia", käsittely on oletuksena kielletty ja siihen on saatava sopimuksen puuttuessa nimenomainen suostumus. Ja koska WP 29 toteaa toisaalla ohjeistus-

luonnoksessa, että online-mainonta voi tietyissä tapauksissa aiheuttaa tällaisia vaikutuksia, voisi tällainen tulkinta esimerkiksi tehdä laittomaksi ilman suostumusta tehdyn automaattisen hinta-erottelun online-markkinoinnissa.

Ja tämähän ei ole sitä, mitä GDPR asiasta sanoo – kyseisessä artiklassa kyse on oikeudesta eikä kiellosta ja näiden ero on perustavanlaatuinen. Jos lainsäätäjä olisi tarkoittanut artiklan kielloksi, olisi kohta kirjoitettu eri muotoon, aivan kuten muualla GDPR:ssä on tehty. Kysymys onkin jälleen siitä, onko tämä mitä GDPR todella sanoo vai pelkästään WP29 lainvastainen tulkinta?

6. Alaikäisten tietojen käsittely edellyttää aina suostumusta

Asetuksesta ei ole tulossa mitään yleistä velvollisuutta hankkia suostumusta alaikäisten tietojen käsittelemiseen. Velvollisuus suostumuksen hankkimiseen alle 16 –vuotiaiden (minimissään 13 –vuotiaiden) huoltajalta tulee vain silloin, jos kyse on tietoyhteiskunnan palvelusta ja käsittelyperusteena on suostumus.

Pia Pynnä
Lakimies
ASML

11 GDPR-vinkkiä markkinoijalle

1. EU:n tietosuoja-asetus vahvistaa merkittävästi kuluttajan oikeuksia päättää itseensä liittyvien henkilötietojen käsittelystä. Asetus antaa hänelle myös entistä suuremman vallan vaatia täydellistä markkinointikieltoa. Markkinoijan kannattaa olla uuden regulaation edessä nöyrä ja kertoa asiakkaalle tämän oikeuksista. On myös valmistauduttava vastaamaan nopeasti erityyppisiin datapyyntöihin ja tiedusteluihin.

2. GDPR on johdonmukainen jatkumo EU:n nykyiselle tietoturvasäännökselle, joten jos noudatat nykyistä säännöstöä, ei suuria muutostöitä välttämättä tarvita. Jos et vielä tätä lukiessasi ole käynnistänyt GDPR-prosessiasi, kannattaa pitää kiirettä.

3. Selvitä aluksi, minkä tyyppistä henkilötietoa yrityksessä on ja missä järjestelmissä sitä ylläpidetään. Arvioi, onko henkilötiedon säilyttäminen ja käyttäminen jonkin uuden tietosuoja-asetuksen käsittelyperusteen mukaisesti hyväksyttyä. Jos asiasta ei ole varmuutta tai tiedot eivät ole liiketoiminnan kannalta tärkeitä, harkitse datasi suursiivousta.

4. Jos olet epävarma siitä, onko kyse tietosuoja-asetuksen tarkoittamasta henkilötiedosta (personally identifiable information, PII), lähde varmuuden vuoksi siitä, että on. Asetus koskee henkilötietoa tai tietoa, joka yksin tai yhdessä muun informaation kanssa, voi johtaa yksilön henkilöllisyyden tunnistamiseen.

5. Henkilötietoihin liittyvät käytännöt, prosessit ja järjestelmät tulisi dokumentoida kattavasti ja läpinäkyvästi, sillä muuten hyvän markkinointitavan kouluttaminen henkilöstölle ei onnistu. Lisäksi on voitava todentaa viranomaisille, että tarpeelliset keinot ja turvamekanismit henkilötietojen suojaamiseksi ovat olemassa.

6. Uuden tietosuoja-asetuksen mukaan kuluttajan suostumuksen saaminen on vain yksi peruste kuudesta käsitellä henkilötietoja. Selvitä, onko tuo suostumus ainoa sinun tilanteeseesi soveltuva peruste. Eduksi on, jos henkilötietojen käsittelyyn on muitakin perusteita, sillä vastedes kuluttaja voi helposti ja tehokkaasti peruuttaa suostumuksensa pysyvästi.

7. Sitouta omaan GDPR-projektiisi sekä IT-osaajat että kaikki saatavilla oleva oikeudellinen asiantuntemus. Asetus takaa kuluttajalle monia oikeuksia, mikä edellyttää markkinoijalta syvää järjestelmäosaamista. Valmistaudu vastaamaan ainakin seuraaviin kysymyksiin:

    - Miten voit taata, että asiakkaan vaatimuksesta hänen henkilötietonsa saadaan tehokkaasti poistettua jokaisesta järjestelmästä ja tietokannasta, johon se on saattanut tietojärjestelmissäsi päätyä?
    - Miten on järjestettävissä, että asiakkaalle tai hänen osoittamalleen kolmannelle osapuolelle voidaan pyynnöstä helposti siirtää koko asiakkaan data luettavissa olevassa formaatissa? Asiakasmäärien ollessa suuria manuaaliset prosessit tulevat kalliiksi.

8. Vastuu tietosuoja-asetuksen noudattamisesta ei rajaudu vain omaan organisaatioosi. Rekisterinpitäjänä (Data Controller) olet vastuussa myös käyttämistäsi alihankkijoista, jotka käsittelevät dataa (Data Processor). Siksi on tärkeää tehdä auditoinnin mahdollistavat sopimukset dataasi käsittelevien yhteistyökumppaneiden kanssa. Kumppaneita voivat olla esimerkiksi painotalot, palvelimien ylläpitäjät tai vaikkapa markkinointiteknologiapalvelujen toimittajat.

9. Asetuksen rikkomiseen liittyvistä sanktioista ja enintään 20 miljoonan euron sakoista on puhuttu paljon. Liiketoimintasi kannalta pahin sanktio olisi kuitenkin todennäköisesti se, että asiakkaasi päättäisivät käyttää oikeuttaan tietojensa poistamiseen ja siihen, ettei heitä koskaan vastaisuudessa saa lähestyä (Right to be forgotten). GDPR-projektiasi ei pelasta mikään, josset markkinoijana ja viestijänä menesty uudessa säänteLyn ympäristössä.

10. Etsi tietosuoja-asetuksesta uusia strategisia mahdollisuuksia. Selvitä voitko hyötyä siitä, että kuluttaja voi vastedes milloin tahansa irtautua asiakassuhteestaan ilman pelkoa itselleen tärkeän datan häviämisestä. Tällöin hänellä on halutessaan mahdollisuus myös tuoda datansa uuteen asiakassuhteeseen.

11. Mieti myös, onko jokin tieto jatkossa viisaampaa anonymisoida tai käsitellä niin, ettei siitä synny tarkkaan säädeltyä henkilötietoa.

Ben Ottoman
Johtaja, tietosuoja
Avaus Marketing Innovations