



1.1.2018

Muistilista

GDPR:n vaikutus markkinointiin



Lähde: World Federation of Advertisers
JULKAISIJA: MAINOSTAJIEN LIITTO

SISÄLLYSLUETTELO

Johdanto	1
Yleistä tietosuojasetuksesta	1
GDPR:n merkitys mainostajille	1
Nämä sinun on hyvä tietää	2
Suostumus.....	2
Suostumuksen osoittaminen.....	3
Oikeutettu etu	3
Läpinäkyvyys.....	4
Lasten henkilötietojen käsittely	5
Henkilötietojen uudelleenkäyttö toiseen tarkoitukseen.....	6
Toimenpidelista	6
muistathan myös nämä!	7
Osoitusvelvollisuus	7
Tietosuojavastaava.....	7
Kuluttajien oikeudet.....	7
Tietoturvaloukkauksista ilmoittaminen.....	8
Sanktiot	8
selitykset ja täsmennykset	8

JOHDANTO

Toukokuun 25. päivä 2018 voimaan astuva EU:n yleinen tietosuoja-asetus (GDPR) edellyttää jokaiselta kuluttajien henkilötietoja keräävältä tai käsittelevältä yritykseltä ja organisaatiolta muutoksia toiminnassaan. Asetuksella on suuri vaikutus mainostajiin, jotka käyttävät kuluttajien henkilötietoja kohdistetuissa markkinointikampanjoissa.

Yleinen tietosuoja-asetus koskee kaikkia yrityksiä, jotka tarjoavat tavaroitaan tai palveluitaan kuluttajille Euroopan Unionin alueella tai seuraavat EU:n kansalaisten käyttäytymistä¹. Asetus siis koskee kansainvälisiä yrityksiä, vaikka niiden pääkonttorit sijaitsevat Euroopan ulkopuolella.

Mainostajien Liitto on tuottanut tämän GDPR-ohjeistuksen kattojärjestönsä WFA:n tuottaman ohjeistuksen pohjalta yhdessä asianajotoimisto Eversheds Sutherlandin kanssa. Alkuperäisen lähteenä olleen ohjeistuksen on tuottanut Huntington & Williams -asianajotoimisto yhdessä WFA:n kanssa. Ohjeet nostavat esiin tietosuoja-asetuksesta tärkeimpiä asioita, jotka mainostajien tulee huomioida.

Tämä ohjeistus tarjoaa konkreettisia neuvoja mainostajille, siitä kuinka tietosuoja tulee lähestyä yleisen tietosuoja-asetuksen valossa. Ohjeistus ei ole kaiken kattava, vaan sen tarkoitus on korostaa muutamia mainostajille tärkeitä tietosuoja-asetuksen osa-alueita. Mainostajat voivat ohjeita apuna käyttäen aloittaa uusien lähestymistapojen suunnittelun ja aloittaa keskustelut tietosuojan kehittämisestä eri asiantuntijoiden kanssa (esimerkiksi lakimiehet, digitaalisesta liiketoiminnasta sekä strategioista vastaavat asiantuntijat). Tämän ohjeistuksen tarkoitus tehtävä on täydentää tietoja, ei toimia laillisesti pätevänä neuvonantona tai toimia sellaisen korvikkeena.

YLEISTÄ TIETOSUOJA-ASETUKSESTA

EU:n yleinen tietosuoja-asetus muuttaa merkittävästi nykyistä tietosuojalainsäädäntöä. Tietosuoja-asetus astuu voimaan 25. toukokuuta 2018 ja koskee kaikkia organisaatioita, jotka Euroopan unionin alueella keräävät henkilötietoja tai seuraavat Euroopan kansalaisten käyttäytymistä. Tietosuoja-asetus koskee kaiken kokoisia ja tyyppisiä organisaatioita, jotka käsittelevät henkilötietoja. Brändin omistajan näkökulmasta tietosuoja-asetus tulee muuttamaan laajalti sitä, miten brändit kommunikoivat kuluttajien kanssa tietosuoja-asioista. Tämä puolestaan tulee rajoittamaan kuluttajien henkilötietojen hyödyntämistä markkinoinnissa. GDPR:ää täydentämään tulee ePrivacy-asetus, joka keskittyy sähköiseen viestintään.

GDPR:N MERKITYS MAINOSTAJILLE

1. Yleinen tietosuoja-asetus tulee muuttamaan merkittävästi sitä, miten ja milloin yritykset voivat käsitellä kuluttajien henkilötietoja.

Eurooppalaista tietosuojalainsäädäntöä pidetään yleisesti maailman tiukimpana. Tietosuoja-asetus lujittaa tätä käsitystä vahvistamalla kuluttajien tietosuoja entisestään. Tietosuoja-asetus kiinnittää entistä tarkempaa huomiota kuluttajien antaman suostumuksen ehtoihin. Lisäksi yrityksille asetetaan tiukkoja vaatimuksia siitä, miten niiden tulisi selvittää kuluttajille mihin yritykset heidän henkilötietojaan käyttävät.

2. Yleinen tietosuoja-asetus tulee vaikuttamaan miltei kaikkiin monikansallisiin suuryrityksiin.

Tietosuoja-asetus koskee kaikkia yrityksiä ja organisaatioita, jotka tarjoavat tavaroitaan tai palveluitaan kuluttajille Euroopan unionin alueella tai jotka seuraavat Euroopan unionin jäsenmaiden kansalaisten käyttäytymistä. Asetus

koskee toisin sanoen suurinta osaa kansainvälisistä yrityksistä, vaikka niiden pääkonttorit sijaitsevat Euroopan ulkopuolella.

3. Tietosuoja-asetuksen laiminlyöminen voi johtaa suuriin sakkoihin.

Sanktiona tietosuoja-asetuksen laiminlyömisestä voidaan antaa sakko, joka voi suuruudeltaan olla jopa 4 % yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Global 500 -listan yritysten sakot voivat siten vaihdella 836 miljoonan ja 19,2 miljardin dollarin välillä. Hallinnollisten sakkojen lisäksi tietosuoja-asetus antaa kuluttajille mahdollisuuden nostaa kanteen yrityksiä vastaan tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä.

NÄMÄ SINUN ON HYVÄ TIETÄÄ

SUOSTUMUS

Yleisessä tietosuoja-asetuksessa on kiinnitetty erityisesti huomiota kuluttajien oikeuksiin päättää, miten yritykset voivat käyttää heidän henkilötietojaan. Monet yritykset käyttävät suostumusta yhtenä monista oikeusperusteista, joihin he vetoavat käsitellessään kuluttajien henkilötietoja. Yleisen tietosuoja-asetuksen myötä edellytykset laillisesti pätevälle suostumukselle tulevat kuitenkin uudistumaan ja laajentumaan.

Useimpien tapausten kohdalla tämä tulee todennäköisesti tarkoittamaan sitä, että kuluttajan suostumusta on kysyttävä **useammin**. Tämä johtuu siitä, että yrityksen on jatkossa kysyttävä suostumusta jokaista erillistä henkilötietojenkäsittelyn käyttötarkoitusta varten. Nämä vaatimukset voivat häiritä kuluttajan asiakaskokemusta verkossa johtaen ärsyyntymiseen tai joissain tapauksissa suostumuksen antamisesta kieltäytymiseen.

Monien tapausten kohdalla saattaa myös olla, ettei palveluun kirjautumisen yhteydessä yleisen luvan antaminen laatikkoa rastittamalla enää riitä suostumukseksi. Uusien sääntöjen mukaan kuluttajan suostumuksen tulee olla **vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen**. Suostumus annetaan joko suostumusta ilmaisevalla lausumalla tai toteuttamalla selkeästi suostumusta ilmaiseva toimi.

Vapaaehtoinen

Kuluttajia ei voida pakottaa antamaan suostumustaan henkilötietojensa keräämiseen ja käsittelyyn palveluun kirjautuessaan, elleivät tiedot ole välttämättömiä palvelun toimimisen kannalta.

Yksilöity

Usein luvan saaminen moniin eri käyttötarkoituksiin vaatii enemmän kuin tietosuojaselosteeseen linkitetyn laatikon rastittamista. Kuluttajien tulee erillisesti antaa suostumuksensa kutakin eri käyttötarkoitusta varten.

Tietoinen

Yritysten tulee jatkossa antaa kuluttajille enemmän tietoa siitä, miten ja mihin tarkoitukseen heidän henkilötietojensa käytetään. Lisäinformaatiota kuluttajille annettavista tiedoista on kappaleessa 3: Läpinäkyvyys.

Yksiselitteinen

Suostumuksesta tulee selkeästi käydä ilmi, että kuluttajat hyväksyvät henkilötietojensa käytön. On hyvin epätodennäköistä, että nk. passiivisten keinojen katsottaisiin olevan yksiselitteisiä ja riittäviä. (Esimerkiksi kuluttajien jatkaessa verkkosivujen käyttöä lukematta tietosuojaselostetta.)

SUOSTUMUKSEN OSOITTAMINEN

Yritysten tulee kyetä osoittamaan saaneensa kuluttajien suostumukset tavalla, joka täyttää nämä edellytykset myös silloin, kun henkilötiedot on kerännyt kolmas osapuoli. Yrityksen markkinoijien ja lakimiesten on siis varmistettava yrityksen yhteistyökumppanien ja muiden kolmansien osapuolten kanssa, että edellytykset täyttyvät.

Suurimmassa osassa tapauksista tarvitaan **nimenomainen suostumus** suorittaessa yksityiskohtaisempaa asiakasprofilointia. Nimenomaisella suostumuksella tarkoitetaan sitä, että kuluttajalle täytyy antaa mahdollisuus suostua tai kieltäytyä henkilötietojensa käytöstä määrättyissä yhteyksissä. Suostumus tulee lisäksi antaa selkeällä tahdonilmaisulla joko suullisesti tai kirjallisesti.

Nimenomainen suostumus on myös edellytys käsiteltäessä henkilötietoja, jotka luokitellaan yleisessä tietosuojasetuksessa ”erityisiin henkilötietoryhmiin” (arkaluonteiset henkilötiedot). Näitä tietoja pidetään luonteeltaan erityisen arkaluontoisina ja niihin kuuluvat:

- Henkilötiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys.
- Geneettiset² tai biometriset³ tiedot, joista henkilön voi yksiselitteisesti tunnistaa
- Terveystta⁴, seksuaalista käyttäytymistä tai seksuaalista suuntautumista koskevat tiedot. Rikostuomioihin tai rikkomuksiin liittyvät tiedot.

TOIMENPITEET:

- ✓ Digitaalisen materiaalin uudelleenarviointi lakimiesten kanssa ja asiakaspinnan päivittäminen vastaamaan tarpeen mukaan uusia suostumuksen edellytyksiä.
- ✓ Mahdollisten yhteistyökumppanien tai muiden kolmansien osapuolten kanssa tehty arviointi henkilötietojen käsittelytavoista, jotta tietosuojasetusta noudatettaisiin.

OIKEUTETTU ETU

Suostumus ei ole ainoa oikeusperuste, johon yritykset voivat vedota käsitellessään henkilötietoja. Yleinen tietosuojasetus sallii tarpeen niin vaatiessa henkilötietojen käsittelyn ilman suostumusta, jos kyse on yrityksen ”oikeutettujen etujen toteutumisesta”.

Tämä on keskeistä erityisesti niiden tapausten kohdalla, joissa suostumuksen saaminen kuluttajilta ei ole mahdollista, esimerkiksi, jos yrityksellä ei ole suoraa yhteyttä kuluttajiin.

Joissakin tapauksissa yritykset voivat perustella kuluttajien henkilötietojen käsittelyä vetoamalla oikeutettuihin etuihinsa, kunhan eduilla ja henkilötietojen käsittelyllä on asiaankuuluva ja relevantti yhteys toisiinsa.

Vedotakseen oikeutettuihin etuihin mainostajien on kuitenkin yhdessä lakimiesten kanssa tehtävä oikeudellisista riskeistä arvio, jossa otetaan huomioon:

- Yrityksen oikeutettujen etujen painoarvo verrattuna kuluttajien yksityisyydensuojaan tai muihin perusoikeuksiin.
- Voivatko kuluttajat kohtuudella odottaa heidän henkilötietojensa käytettävän näissä tapauksissa perustuen heidän ja yrityksen väliseen suhteeseen.

Oikeutettuihin etuihinsa vetoavien yritysten on myös selitettävä nämä edut kuluttajille esimerkiksi tietosuojaselosteessaan.

Mainostajien tulisi siis selvittää yhdessä lakimiesten kanssa, onko yrityksellä oikeusperustetta käsitellä henkilötietoja tietyissä yhteyksissä⁵.

TOIMENPITEET:

- ✓ Tapauskohtainen arviointi lakimiesten kanssa siitä, onko suostumus tarpeellinen kerätessä kuluttajien henkilötietoja markkinointikampanjoiden kautta.

LÄPINÄKYVYYS

Läpinäkyvyys kuuluu EU:n tietosuojalainsäädännön pääperiaatteisiin ja yleinen tietosuoja-asetus tuo mukanaan uusia läpinäkyvyyttä koskevia velvoitteita yrityksille. Tietosuoja-asetus velvoittaa yrityksiä informoimaan kuluttajia siitä, mihin tarkoitukseen he käyttävät tai aikovat käyttää kuluttajien henkilötietoja. Henkilötietojenkäsittelystä annetun informaation tulee olla helposti ymmärrettävissä ja helposti saatavilla olevassa muodossa sekä selkeää ja yksinkertaista kieltä.

Nämä vaatimukset luovat mainostajille haasteita, kun yhtäältä kuluttajille on annettava enemmän tietoa, toisaalta annettu tieto ei saisi olla vaikeasti ymmärrettävää tai määrällisesti liiallista. Mainostajien tulee käyttää luovuuttaan yrittäessään sisällyttää kaikkea tätä tietoa henkilötietoja hyödyntäviin digikampanjoihinsa.

WFA järjesti helmikuussa 2017 jäsenyrityksilleen Digital Governance Exchange -työpajan (DGX), jossa mm. jaettiin yhdessä ideoita ja käytännön toteutuksia liittyen tietosuoja-asetuksen vaikutuksiin. Työpajalla selvitettiin miten, missä ja milloin tietoja tulisi parhaiten kerätä, jotta kuluttajille välitettävä tieto olisi silti läpinäkyvää ja kuluttajien omiin henkilötietoihin liittyvät valinnanvapaudet ja hallintaoikeudet säilyisivät. Työpajan avulla nostettiin esiin kuusi pääohjetta, joista voi olla hyötyä pohdittaessa kuinka läpinäkyvyyttä voidaan lisätä käytännössä.

Visualisoi

- Emoji-idea: käytä tietosuojaselosteessa helposti ymmärrettäviä symboleja, esim. ikoneja, luottamusmerkintöjä ja sinettejä.
- Hyödynnä lyhyitä videoita tekstien sijaan.

Selitä lyhyesti ja yksinkertaisesti

- Käytä vain kieltä, jota 13-vuotiaskin ymmärtäisi.
- Kerro vain olennaisesta.
- Nosta esiin vain huomionarvoiset seikat ja anna kuluttajalle mahdollisuus klikata lukeakseen enemmän.

Älä häiritse

- Kysy suostumusta vain tarvittaessa.
- Älä ole päällekkävyä tai häiritse asiakaskokemusta.

Anna mahdollisuus muuttaa mieltä

- Anna käyttäjille helppokäyttöinen järjestelmä, jolla he voivat muokata kaikkia yksityisyysasetuksiaan yhdessä paikassa. Esim. tehtäväpalkit, ohjauspaneelit, ilmoituskeskukset.
- "Kadun päätöstäni" -painike: anna käyttäjille mahdollisuus muuttaa halutessaan mieltään milloin vain.

Helpota asioita

- Tee pois pääsystä helpompaa kuin sitoutumisesta.
- Helpota käyttäjän suostumista tai kieltäytymistä esimerkiksi käyttämällä sormen pyyhkäisyä klikkauksen sijaan.

Kerro aikeistasi

- Kysyessäsi henkilötietoja selitä käyttäjille, miksi tarvitset niitä.
- Selitä suostumuksen ja kieltäytymisen seuraamukset.
- Kerro selkeästi mitä kuluttaja hyötyy vaihtokaupasta, esimerkiksi yksi musiikkivideo vastaa 10 sekunnin mainosta.

TOIMENPITEET

- ✓ Tietosuojainformaatiota koskevien luovien ratkaisujen löytäminen verkkokampanjoihin ja muihin digitaalisiin sovelluksiin.

LASTEN HENKILÖTIETOJEN KÄSITTELY

Jos lapsen henkilötietoja käsitellään tietoyhteiskunnan palvelujen kuten esimerkiksi verkkopalvelujen tarjoamiseksi suostumuksen perusteella, tarvitaan vanhemman suostumus⁶. Kun henkilötietoja käsitellään suostumuksen perusteella ja kyseessä on tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle, lapsen henkilötietojen käsittely on Suomessa lainmukaista, jos lapsi on vähintään 13-vuotias tai lapsen vanhempainvastuunkantajalta on saatu asianmukainen suostumus tai valtuutus henkilötietojen käsittelemiseksi.

Yritysten tulee tästä syystä ratkaista teknisesti, miten ne aikovat kysyä ja vahvistaa vanhemman suostumuksen. EU:n jäsenvaltiot voivat omassa lainsäädännössään määrittää ikärajan 13-16 ikävuoden välille ja yrityksen on syytä varautua, että ikäraja voi vaihdella eri EU-maissa, joissa se toimii.

Yleinen tietosuoja-asetus ei määrittele erityisen tarkasti, miten vanhemman suostumus määritellään päteväksi. Lapsille tavaroita tai palveluita markkinoivien yritysten olisikin viisainta laittaa liikkeelle viestintä- tai lakiasioista vastaavat selvittämään tietosuojaviranomaisen avustuksella, kuinka lasten henkilötietojen käsittelyyn liittyvät toimenpiteet tulisi toteuttaa.

TOIMENPITEET:

- ✓ Jokaisen lapsen henkilötietoja käyttävän kampanjan ja/tai digitaalisen sovelluksen uudelleenarviointi. Arvioinnissa tulee ottaa huomioon 13 vuoden ikäraja ja mahdollinen tarve vanhemman suostumukselle.

HENKILÖTIETOJEN UUELLEENKÄYTTÖ TOISEEN TARKOITUKSEEN

Monissa tapauksissa henkilötietoja kerätään yhtä tiettyä käyttötarkoitusta, esim. uutiskirjeen tilausta varten. Mainostajia saattaa kuitenkin kiinnostaa samojen henkilötietojen käyttäminen asiakasymmärryksen kehittämistarkoituksessa. Tällöin he voisivat hyödyntää tietoja uudestaan mainoskampanjoissaan tai kohdistettaessa samankaltaisia markkinointiviestejä muista tuotteista tai palveluista.

Jos suostumuksen pyytäminen uudelleen ei ole mahdollista tai soveliaista, täytyy mainostajien yhdessä lakimiesten kanssa arvioida, voiko henkilötietoja käyttää toisiin käyttötarkoituksiin ilman suostumusta.

Arvioinnissa tulee ottaa huomioon seuraavat tekijät:

- ✓ Yhteys henkilötietojen keräämisen alkuperäistarkoituksen ja tulevan käyttötarkoituksen välillä.
- ✓ Konteksti, jossa henkilötiedot on alun perin kerätty.
- ✓ Kuluttajien kohtuulliset odotukset, jotka perustuvat heidän suhteeseensa yrityksen kanssa.
- ✓ Henkilötietojen arkaluonteisuus
- ✓ Henkilötietojen hyödyntämisestä uudessa käyttötarkoituksessa johtuvat mahdolliset seuraukset.
- ✓ Onko henkilötietoja tehty nimettömiksi, salattu tai suojattu muilla tavoin.

TOIMENPITEET:

- ✓ Jos aikomuksena on käyttää aiemmin kerättyjä henkilötietoja uusiin käyttötarkoituksiin, on parasta tarkistaa lakimiehiltä, onko tämä mahdollista.

TOIMENPIDELISTA

Yleisen tietosuojasetuksen astuessa voimaan 25. toukokuuta 2018 mainostajien tulee varautua tässä ohjeistuksessa esiin nostettuihin muutoksiin. Mainostajien tulisi tulevaan valmistautuessaan harkita vähintään seuraavia jatkotoimenpiteitä:

- ✓ Tietosuojainformaatiota koskevien luovien ratkaisujen löytäminen verkkokampanjoihin ja muihin digitaalisiin sovelluksiin.
- ✓ Digitaalisen materiaalin uudelleenarviointi lakimiesten kanssa ja asiakkaiden kontaktipisteiden päivittäminen vastaamaan tarpeen mukaan uusia suostumuksen edellytyksiä.
- ✓ Jokaisen lasten henkilötietoja käyttävän kampanjan ja/tai digitaalisen sovelluksen uudelleenarviointi. Arvioinnissa tulee ottaa huomioon 13 vuoden ikäraja ja mahdollinen tarve vanhemman suostumukselle.
- ✓ Tapauskohtainen arviointi lakimiesten kanssa siitä, onko suostumus tarpeellinen kerätessä kuluttajien henkilötietoja markkinointikampanjoiden yhteydessä.
- ✓ Jos aikomuksena on käyttää aiemmin kerättyjä henkilötietoja uusiin käyttötarkoituksiin, on parasta tarkistaa lakimiehiltä, onko tämä mahdollista.
- ✓ Mahdollisten yhteistyökumppanien tai muiden kolmansien osapuolten kanssa tehty arviointi henkilötietojen käsittelytavoista, jotta tietosuojasetusta noudatettaisiin.

MUISTATHAN MYÖS NÄMÄ!

Seuraavassa osiossa käsitellään lukuisia muita yleiseen tietosuoja-asetukseen liittyviä seikkoja. Niillä ei ehkä ole erityisen suoraa vaikutusta juuri mainostajiin, mutta ne ovat silti huomionarvoisia koko yrityksen näkökulmasta. Suosittelemme kääntymistä lakimiesten puoleen, mikäli seuraavien seikkojen toteuttamisesta herää lisäkysymyksiä.

OSOITUSVELVOLLISUUS

Yritysten tulee toimenpiteillään osoittaa, että he noudattavat tietosuoja-asetusta.

TIETOSUOJAVASTAAVA

Joidenkin yritysten on nimitettävä tietosuojavastaava valvomaan tietojenkäsittelyyn liittyvää toimintaa. Vaatimus pätee kaikkiin yrityksiin, joiden ydintehtäviin sisältyy:

- Laajamittainen ja systemaattinen henkilöiden käyttäytymisen seuranta.
TAI
- Laajamittainen tietojenkäsittely koskien erityisiin henkilötietoryhmiin kuuluvia tietoja taikka rikostuomioihin tai rikkomuksiin liittyviä tietoja.
- Yritysten tulee yllä mainitun jaottelun perusteella määritellä ovatko ne lain mukaan velvollisia nimittämään tietosuojavastaavan⁷.

Yritysten on luotava kansainvälisesti toimiva järjestelmä, jonka avulla voidaan suorittaa tietosuoja koskeva vaikutusten arviointi. Tämä on tehtävä ennen kuin käsitellään henkilötietoja, joihin sisältyy korkea tieturvariski⁸. Markkinoijien ja lakimiesten tulisi yhteisymmärryksessä selvittää, milloin ja miten tietosuoja koskeva vaikutusten arviointi tulisi toteuttaa tulevia projekteja varten.

Yritysten täytyy myös ylläpitää viranomaisia varten kirjallista selostetta tietojenkäsittelytoimistaan. Velvollisuus ei välttämättä koske alle 250 työntekijän yrityksiä (tietyillä edellytyksillä). Tietosuoja-asetuksessa mainitaan lista selosteeseen sisällytettävistä tiedoista. Velvollisuus laatia seloste käsittelytoimista liittyy osoitusvelvollisuuden toteuttamiseen.

Yritykset, joiden kotipaikka on EU:n ulkopuolella, on nimettävä itselleen edustaja jossain EU:n jäsenvaltiossa. Edustajan tehtäviin kuuluu yhteydenpito tietosuojaviranomaisen kanssa.

KULUTTAJIEN OIKEUDET

Yritysten tulee toteuttaa asianmukaisia teknisiä järjestelyitä, joilla varmistetaan kyky vastata kuluttajien henkilötietoihin liittyviin pyyntöihin. Kuluttajilla on oikeus pyytää pääsyä omiin henkilötietoihinsa ja tämän lisäksi myös oikeus pyytää tietojensa poistamista, oikaisemista tai luovuttamista (tietyin edellytyksin). Tietyissä tilanteissa kuluttajilla on myös oikeus vastustaa henkilötietojensa käsittelyä tai pyytää tietojaan annettavaksi takaisin heille. Kuluttajilla on niin ikään myös oikeus pyytää henkilötietojensa siirtämistä toisen yrityksen järjestelmään. Yritysten on valmistauduttava vastaamaan kaikkiin kuluttajien pyyntöihin ”ilman aiheetonta viivytystä” ja päivittämään tietojärjestelmänsä ajan tasalle toteuttaakseen pyynnöt.

TIETOTURVALOUKKAUKSISTA ILMOITTAMINEN

Kaikista henkilötietoon kohdistuvista tietoturvaloukkauksista (esim. tietovuodoista ja -murroista) tulee ilmoittaa 72 tunnin kuluessa toimivaltaiselle tietosuojaviranomaiselle. Joissakin tapauksissa tietoturvaloukkauksista pitää ilmoittaa lisäksi kuluttajille suoraan. Lyhyt määräaika edellyttää yrityksiltä nopeaa reagoitakykyä epäiltyjen tietoturvaloukkausten ilmetessä. Reagoitakyvyllä voi olla myös vaikutusta brändien maineelle.

Mainostajien tulisi harkita yhteistyötä lakimiesten, IT-osaston ja muiden liiketoimintayksiköiden kanssa, jotta he voisivat muodostaa yritykselle viestintästrategian tietoturvaloukkausten varalta. Strategiaan on hyvä sisällyttää keinoja, joiden avulla kuluttajille voitaisiin ilmoittaa tietoturvaloukkauksista suoraan, brändin mainetta mahdollisimman vähän vaarantamalla.

SANKTIOT

Yritysten sakot tietosuoja-asetuksen laiminlyönnistä voivat korkeimmillaan olla 4 % yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta tai 20 miljoonaa euroa, riippuen kumpi summa on korkeampi.

Kuluttajat, yleishyödylliset yhteisöt ja kuluttajia edustavat järjestöt voivat niin halutessaan myös nostaa kanteen yritystä vastaan tietosuoja-asetuksen laiminlyömisestä.

SELITYKSET JA TÄSMENNYKSET

¹ "Käyttötymisen seuranta" voi tarkoittaa esimerkiksi henkilöiden jäljittämistä verkossa.

² Geneettiset tiedot määritellään yleisessä tietosuoja-asetuksessa henkilötietoina, "jotka koskevat luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta".

³ Biometriset tiedot määritellään yleisessä tietosuoja-asetuksessa seuraavasti: "kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa".

⁴ Terveystiedot määritellään yleisessä tietosuoja-asetuksessa seuraavasti: "luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, mukaan lukien tiedot terveyspalvelujen tarjoamisesta, jotka ilmaisevat hänen terveydentilansa".

⁵ Lisätietoja oikeutetuista eduista löytyy englanniksi EU:n 29 artiklan mukaisen tietosuojatyöryhmän lausunnosta 06/2014: *Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*.

⁶ Jos muihin oikeusperusteisiin ei voida vedota, tarkista tämän ohjeistuksen kappale 2: Suostumuksen saamisen ollessa mahdotonta.

⁷ Yritysten on myös arvioitava mitä edellytyksiä tietosuojavastaavalta vaaditaan EU:n jäsenvaltioiden tasolla. Vaikka kaikki yritykset eivät olekaan veloitettuja kriteereiden mukaisesti nimittämään tietosuojavastaavaa, ne voivat silti nimittää tietosuojavastaavan vapaaehtoisesti helpottaakseen tietosuoja-asetuksen noudattamistaan. Vapaaehtoista tietosuojavastaavaa koskevat samat edellytykset kuin tietosuoja-asetuksen määrittelemää tietosuojavastaavaa.

⁸ Tietosuojaa koskeva vaikutusten arviointi on tehtävä aina, kun kyse on tietojenkäsittelyyn liittyvistä yksilöiden oikeuksien ja vapauksien kannalta korkeista riskeistä.

⁹ Yleinen tietosuojasetus määrittelee kaikki henkilötietojen turvallisuuden vaarantumistapaukset ”tietoturvaloukkauksina”, jotka johtavat lähetettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingolliseen tai laittomaan tuhoutumiseen, katoamiseen, muutokseen, luvattomaan julkistamiseen tai luvattomaan pääsyyn henkilötietoihin.

¹⁰ Edeltävän tilikauden.