Building a better working world

Tietosuojakysymyksiin liittyvät säännöt ja määräykset täsmentyvät

EU:n vuonna 2016 vahvistetun ja vuonna 2018 voimaan tulleen yleisen tietosuoja-asetuksen (GDPR) myötä tietosuoja-asiat ovat tulleet osaksi yhä useamman yrityksen arkipäivää. Tietosuoja-asetuksen ja sen seurauksena säädetyn kansallisen tietosuojalain lisäksi on vuonna 2020 annettu tarkentavia linjauksia ja tulkintoja muun muassa tietosuojavaltuutetun ja EU-tuomioistuimen toimesta. Linjaukset ovat liittyneet muun muassa yritysten toimintatapoihin koskien tietosuojaa, tiedon siirtoon EU:n ja Yhdysvaltojen välillä sekä yritysten verkkosivuilla hyödynnettyihin evästeisiin.

Tietosuojarikkomuksista on myös Suomessa määrätty ensimmäiset sanktiot. Yritysten onkin korkea aika varmistua siitä, että tietosuojaan liittyvät toimintatavat ja dokumentaatio ovat ajan tasalla ja lainsäädännön mukaiset.

Suomessa on määrätty ensimmäiset seuraamusmaksut

Tietosuojavaltuutetun toimiston seuraamuskollegio antoi toukokuussa 2020 Suomen ensimmäiset seuraamusmaksut neljälle, tietosuojarikkomuksiin syyllistyneelle yritykselle. Viides seuraamusmaksu määrättiin elokuussa 2020. Yksi seuraamusmaksuun johtaneista tietosuojarikkomuksista johtui lainsäädännön edellyttämän informointivelvoitteen toteuttamisen puutteista. Kyseinen yritys ei muun muassa ollut kertonut asiakkailleen näiden oikeudesta kieltää henkilötietojen luovuttaminen eteenpäin. Siitä seurasi, että asiakkaat joutuivat muiden yritysten suoramarkkinoinnin ja yhteydenottojen kohteiksi. Tietosuojarikkomus kohdistui yhteensä 161 000 asiakkaaseen ja yritykselle määrättiin seuraamusmaksuna 100 000 euroa. Yritysten tuleekin kiinnittää erityistä huomiota siihen, millä tavoin henkilötietojen käsittelystä ja luovutuksista kerrotaan rekisteröidyille, eli esimerkiksi asiakkaille. Lainsäädännön vaatimukset ovat tältä osin melko tiukat.

Tietyin edellytyksin yritykset ovat tietosuojalainsäädännön mukaisesti velvollisia arvioimaan henkilötietojen käsittelyn vaikutuksia. Tällaisessa vaikutustenarvioinnissa tulee arvioida käsittelyn tarvetta, oikeasuhtaisuutta ja niihin liittyviä riskejä. Kahden yrityksen kohdalla tämänkaltaisen vaikutustenarvioinnin puuttuminen johti seuraamusmaksuihin. Yksi seuraamusmaksun saaneista yrityksistä oli käsitellyt työntekijöidensä sijaintitietoja työajanseurantaa varten paikantamalla työntekijöiden ajoneuvoja. Tapaus johti 16 000 euron suuruiseen seuraamusmaksuun. Toinen, myös sijaintitietoja keräävä yritys, oli puolestaan käyttänyt turvakameravalvontaa ja äänen tallentamista taksiautoissa, kuitenkaan kertomatta siitä asiakkaille. Lisäksi taksiyhtiöllä ilmeni useita puutteita informointikäytännössään, dokumentoinnissaan ja henkilötietojen käsittelyn liittyvien roolien määrittelyssään. Tapauksen seuraamusmaksun määrä oli 72 000 euroa. Esimerkiksi kameravalvontaan liittyvät kysymykset saattavat monesti vaatia erityistä huolellisuutta yrityksiltä, vaikka kyseessä olisi ainoastaan toimitilojen turvallisuuteen liittyvä valvonta.

Olennainen vaatimus henkilötietojen käsittelyssä on, että yrityksen tulee pystyä perustelemaan käsittelyn tarpeellisuus tapauskohtaisesti. Mikäli esimerkiksi tietoja työntekijän uskonnollisesta vakaumuksesta tai muusta tarpeettomaksi katsottavasta tiedosta käsitellään, voi tarpeeton käsittely johtaa seuraamuksiin. Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi 12 500 euron suuruisen seuraamusmaksun sen johdosta, että yritys käsitteli tarpeettomia tietoja työntekijöistään ja potentiaalisista työntekijöistä rekrytointivaiheessa.

Viimeisin, elokuussa määrätty seuraamusmaksu liittyi suoramarkkinointiviesteihin, joita yritys lähetti asiakkailleen ilman asiakkaiden ennalta annettua suostumusta. Tältä osin määrätty seuraamusmaksu oli suuruudeltaan 7 000 euroa. Yritysten onkin kiinnitettävä erityistä huomiota myös suoramarkkinointiin liittyvissä toimenpiteissään.

Määrätyt seuraamusmaksut ovat selkeä merkki siitä, että tietosuojaviranomainen on ottanut tietosuojarikkomukset vakavasti ja aktivoitunut lainsäädännön valvonnassa ja tulkinnassa myös Suomessa. Euroopassa eri maiden tietosuojaviranomaiset ovat määränneet jo aiemmin myös huomattavasti suurempia sanktiota.

Evästeisiin liittyvät viranomaisten määräykset ovat täsmentyneet

Evästeet (cookiet) ovat yleisesti käytetty ja kätevä tapa kerätä tietoa mm. verkkosivun vierailijan käyttäytymisestä ja siten kohdistaa henkilön mieltymyksiin kuuluvaa informaatiota ja mainontaa. Evästeiden käyttö edellyttää verkkosivustolla vierailevan henkilön suostumusta, joka tietosuoja-asetuksen mukaan tulee olla vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilö hyväksyy tällaisten henkilötietojen käsittelyn. Aiemmin on yleisesti saatettu käyttää ilmoitusta, ns. banneria, jossa on todettu esimerkiksi että "Jatkamalla sivuston käyttöä hyväksyt evästeiden käytön" tai "Painamalla OK-painiketta hyväksyt evästeet".

Apulaistietosuojavaltuutettu otti kantaa tämänkaltaisiin ilmoituksiin päätöksessään 14.5.2020 ja lausui, että tämänkaltaiset tavat kerätä suostumuksia eivät täytä tietosuoja-asetuksen edellytyksiä pätevästä suostumuksesta. Käyttäjälle ei anneta mahdollisuutta valita itse, hyväksyykö vai hylkääkö hän evästeiden käyttämisen. Käyttäjällä tulisi sen sijaan olla täysi vapaus itse aktiivisella toimellaan hyväksyä evästeiden käyttäminen, esimerkiksi siten, että hän itse rastittaa "OK"-ruudun, tai valitsee "Hyväksyn"-painikkeen "Hylkään"-painikkeen sijasta. Näiden ehtojen lisäksi on varmistettava, että suostumuksen peruuttaminen on yhtä helppoa kuin sen antaminen, ja että suostumusta keräävä banneri ei saa haitata verkkosivun käyttämistä.

Apulaistietosuojavaltuutetun päätös selventää aiemmin hieman täsmentymätöntä oikeustilaa ja suojaa henkilöitä heidän tietämättään tai tahtomattaan tapahtuvasta henkilötietojen keräämisestä. Jokaisen yrityksen tulisikin nyt arvioida evästekäytäntönsä sekä niihin liittyvät ilmoitukset verkkosivuillaan ja päivittää niitä tarvittaessa.

Tietosuoja ja koronavirus

Koronaviruksen seurauksena työnantajat ovat saattaneet tiedustella ja pitää kirjaa esimerkiksi työntekijöiden terveydentilasta ja perheen olosuhteista tavallista herkemmin. Työnantajien ja terveystietoja käsittelevien henkilöiden on silti muistettava käsitellä työntekijöiden terveystietoja lainmukaisesti luottamuksellisesti, oikeasuhtaisesti ja kohtuullisesti. Tämä vaatimus on asetettu lisäksi vahvasti työnantajia velvoittavassa laissa yksityisyyden suojasta työelämässä (ns. työelämän tietosuojalaki). Tämä tarkoittaa esimerkiksi sitä, että työnantaja tai terveystietoja käsittelevä henkilö ovat aina vaitiolovelvollisia, eikä työnantaja lähtökohtaisesti saa nimetä koronaa sairastavaa henkilöä tunnistettavalla tavalla.

Työnantaja ei lähtökohtaisesti voi pakottaa työntekijää koronatestiin, mutta on oikeutettu estämään henkilön työnteon epäillessään hänen sairastavan koronavirusta. Työntekijä voi antaa suostumuksensa terveystietojensa käsittelyyn, keräämiseen ja luovuttamiseen, mutta tällöin suostumuksen tulee täyttää yllä mainitut tietosuoja-asetuksen asettamat vaatimukset ollakseen pätevä.

Yhdysvaltoja koskeva Privacy Shield -järjestely kumottiin heinäkuussa

Niin kutsuttu *Privacy Shield* -järjestely on luonut tietosuojalainsäädännön edellyttämän lähtökohdan tiedon siirtämiselle EU:n ja Yhdysvaltojen välillä. Sen avulla EU:ssa toimivia yrityksiä on pyritty suojaamaan muun muassa Yhdysvaltojen viranomaisten pääsyltä henkilötietoihin. EU-tuomioistuin totesi heinäkuussa 2020 niin kutsutussa Schrems II-päätöksessään, että EU:n tietosuoja-asetuksen voimaan tullessa Privacy Shield -järjestely ei kuitenkaan enää täytä EU:n tietosuojastandardeja. Tästä syystä myöskään henkilötietojen käsittelyn turvallisuus ja tietosuoja ei ole Yhdysvalloissa riittävällä tasolla. Näistä lähtökohdista johtuen EU-tuomioistuin kumosi Privacy Shield -järjestelyn.

Vaikka on helppo ajatella, että kyseinen päätös ei koske omaa yritystä, ei asia valitettavasti ole niin. EU-tuomioistuimen päätös koskettaa lukuisia toimijoita, sillä useat yritykset hyödyntävät Privacy Shield -järjestelyn turvin toimivia palveluntarjoajia. Esimerkiksi monella yleisellä mm. markkinointiin liittyviä palveluita tarjoavalla yrityksellä saattaa olla pääkonttori Yhdysvalloissa, ja tietoja on luovutettu Yhdysvaltoihin kyseisen Privacy Shield -järjestelmän turvin. Yritysten onkin nyt syytä varmistaa, että kyseiset palveluntarjoajat voivat taata lainmukaisen ja turvallisen henkilötietojen siirron käyttäen muita lainsäädännön edellyttämiä suojakeinoja. Suositeltavaa onkin, että organisaatio käy läpi kaikki henkilötietojen käsittelyä koskevat sopimuksensa ja tarkistaa onko niissä annettu henkilötietojen käsittelijälle oikeus käsitellä tietoja EU/ETA-alueen. ulkopuolisissa maissa ja mikäli on, millä ehdoilla ja millä tavoin se toteutetaan.

EY:n asiantuntijat antavat mielellään lisätietoja tietosuoja-asioissa tapahtuvista linjauksista, ja auttavat teitä niitä koskevissa kysymyksissä.

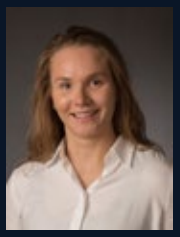
EY | Assurance | Tax | Strategy and Transactions | Consulting

EY lyhyesti
EY on globaali tilintarkastuksen, verotuksen, liikejuridiikan, ja yritysjärjestelyiden asiantuntija ja liikkeenjohdon konsultti. Näkemyksemme ja korkealaatuiset palvelumme vahvistavat luottamusta pääomamarkkinoiden ja talouden toimintaan kaikkialla maailmassa. Kasvatamme huippuosaajia, joiden yhteistyöllä lunastamme lupauksemme ja rakennamme parempaa työ- ja liike-elämää sekä toimivampaa maailmaa asiakkaillemme, omalle henkilöstöllemme ja yhteisöille, joissa toimimme. Lisätietoja löydät internetistä www.ey.com/fi. Voit myös seurata meitä twitterissä: @EY_Suomi.

Lisätietoja organisaatiostamme löytyy osoitteesta ey.com.

Ota yhteyttä

Joe Gummerus
Senior Legal Counsel
p. +358 40 350 7334
joe.gummerus@fi.ey.com



Mira Ahonen
Associate Legal Counsel
p. +358 44 268 1826
mira.ahonen@fi.ey.com

www.ey.com/fi

B20008fi