Kaksi vuotta GDPR:ää – Tietosuojavaltuutetun EU:n yleisen tietosuoja-asetuksen mukaiset päätökset

Kaksi vuotta GDPR:ää –
Tietosuojavaltuutetun EU:n yleisen tietosuoja-asetuksen mukaiset päätökset

Tietosuojavaltuutetun toimisto on julkaissut yhteensä 17 yleisen tietosuoja-asetuksen mukaista päätöstä tietosuoja-asetuksen soveltamisajan aikana. Ensimmäistä kertaa myös seuraamuskollegio, jonka muodostavat tietosuojavaltuutettu ja kaksi apulaistietosuojavaltuutettua, määräsi seuraamusmaksuja tietosuojavelvoitteiden laiminlyönnin seurauksena. Kolmessa tapauksessa määrättiin hallinnollinen seuraamusmaksu. Tietosuojavaltuutettu tai apulaistietosuojavaltuutettu ovat antaneet lisäksi huomautuksen yhteensä seitsemässä tapauksessa. Kaikki päätökset eivät ole vielä lainvoimaisia, ja niistä voi valittaa hallintovalituksena hallinto-oikeuteen. Päätöksissä on ollut kyse muun muassa seuraavista alla lyhyesti kuvatuista tietosuoja-asetuksen asettamista vaatimuksista. Tarkemmat tiivistelmät kaikista päätöksistä löydät liitteenä olevasta tapausten koosteesta.

Rekisteröityä tulee informoida tehokkaasti ja läpinäkyvästi henkilötietojensa käsittelystä.

Tapauksessa, joka johti 100.000 euron hallinnolliseen sanktioon, oli kyse rekisterinpitäjän informointivelvoitteen laiminlyönnistä (*päätös 18.5.2020, Dnro 3818/161/2020*). Informointivelvoitteella tarkoitetaan sitä, että rekisteröidyllä on oikeus saada tietoa hänen henkilötietojensa keräämisestä ja käsittelystä. Henkilötietojen käsittelyn on oltava läpinäkyvää. Käytännössä rekisteröidylle on kerrottava:

- rekisterinpitäjä ja sen yhteystiedot
- käyttötarkoitukset, joihin tietoja käsitellään
- tietojen käsittelyperuste
- tietojen säilytysajoista
- mihin tietoja luovutetaan

- tieto henkilötietojen siirrosta EU:n ja ETA-alueen ulkopuolelle
- rekisteröidyn oikeuksista
- mistä tiedot on saatu silloin, kun ne on saatu muualta kuin rekisteröidyltä itseltään.

Informaatio on annettava selkokielellä tiiviisti esitettynä, ja se tulee olla helposti saatavilla.

Evästeiden osalta suostumusta ei voi pyytää siten, että rekisteröity informoidaan jatkamaan sivustolla käyttöä ilman tosiasiallista valinnan mahdollisuutta.

Suomen tietosuojavaltuutetun toimisto antoi odotetun kansallisia evästekäytäntöjä selkeyttävän päätöksen. Evästeet ovat pieniä tekstitiedostoja, joita tallennetaan käyttäjän päätelaitteelle verkkosivuilla vieraillessa. Evästeitä voidaan hyödyntää esimerkiksi sivujen teknisen toimivuuden varmistamisessa ja markkinoinnin kohdentamisessa. Apulaistietosuojavaltuutettu toi esille tapauksessa (*päätös 14.5.2020, Dnro: 8040/163/2019*), että sivuston evästebannerissa tulee antaa rekisteröidylle mahdollisuus kieltäytyä evästeiden tallentamisesta ja niiden käyttämisestä. Suostumusta ei voida pyytää rekisteröidyltä ohjaamalla hänet muuttamaan evästeitä koskevat käytännöt selainasetusten kautta. Suostumuksen on oltava vapaaehtoisesti ja tietoisesti annettu sekä yksilöity tiettyyn käyttötarkoitukseen. Suostumuksen tulee olla peruutettavissa yhtä helposti kuin se on annettu.

Vaikutustenarviointi on tehtävä, kun suunniteltu käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.

Hallinnolliseen seuraamusmaksuun (16.000 euroa) johtava päätös (*18.5.2020 Dnro 531/161/20*) koski vaikutusten arviointia, jonka tekeminen oli laiminlyöty ajotietojärjestelmään liittyvän henkilötietojen käsittelyn osalta. Tapauksessa työntekijän sijaintietoja käsiteltiin työajanseurantaa varten. Käytännössä rekisterinpitäjän olisi tullut tehdä vaikutusten arviointi. Velvoite tehdä vaikutustenarviointi seuraa tietosuoja-asetuksessa yksilöityjen käsittelytilanteiden johdosta tai siitä, että käsittelytoimenpide on lisätty tietosuojaviranomaisen luetteloon taikka kansallisesta lainsäädännöstä. Vaikutustenarviointi on tehtävä esimerkiksi silloin, kun käsittelyssä käytetään uutta teknologiaa ja henkilötietojen käsittelyn käyttötarkoitus on rekisteröityjen tarkkailu tai seuranta. Lisäksi kun on kyse esimerkiksi rekisteröidyn työsuorituksen tai käyttäytymisen, sijainnin tai liikkumisen arvioinnista tai pisteytyksestä. Tämä koskee erityisesti heikossa asemassa olevia rekisteröityjä, kuten työntekijöitä, koska rekisteröidyn voi olla vaikeaa vastustaa tietojensa käsittelyä tai käyttää muita oikeuksiaan. Vaikutusten arviointi on tehtävä rekisteröidyn näkökulmasta arvioiden mitä rekisteröidyn oikeuksia ja vapauksia käsittely saattaa vaarantaa, sekä millaisia vahinkoja rekisteröidyille voi aiheutua. Rekisteröidyille koituvat vahingot voivat olla fyysisiä, aineellisia tai aineettomia. Esimerkkeinä vahingoista on rekisteröidyn terveyden vaarantuminen, maineen menetys, mielipaha, syrjintä tai identiteettivarkaus.

Jos rekisteröityjä ei voi tavoittaa tietoturvaloukkauksen johdosta, rekisterinpitäjän tulee käyttää julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille voidaan tiedottaa tietoturvaloukkauksesta tehokkaasti.

Kahdessa huomautuksiin johtaneessa tapauksessa (*päätökset 10.10.2019, Dnro 2691/171/19 ja 3.1.2020, Dnro 60/171/2020*) otettiin kantaa tietoturvaloukkauksesta ilmoittamiseen rekisteröidylle. Tapauksissa ilmoittamista ei oltu tehty riittävän tehokkaasti. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos loukkaus todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Ilmoitusvelvollisuus mahdollistaa sen, että rekisteröidyt voivat suojautua loukkaukselta ja sen vaikutuksilta esimerkiksi sulkemalla

luottokortin tai vaihtamalla käyttäjätilin salasanan. Jos kaikkia rekisteröityjä ei voi tavoittaa henkilökohtaisesti tietoturvaloukkauksen johdosta, rekisterinpitäjän tulisi käyttää julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille voidaan tiedottaa tietoturvaloukkauksesta tehokkaasti. Tietyissä tietosuoja-asetuksen mukaisissa erikseen mainitussa tilanteissa ilmoitusta ei vaadita.

Työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja.

Tapauksessa, jossa määrättiin myös 12.500 euron suuruinen hallinnollinen seuraamusmaksu (*asia 20.5.2020 Dnro 137/161/20*), oli kyse työnhakijoiden tietojen laittomasta käsittelystä. Rekisterinpitäjä oli kysynyt tietoja työnhakijoilta mm. uskonnollisesta vakaumuksesta, terveydentilasta, mahdollisesta raskaudesta ja perhesuhteista. Käytännössä tietoja oli käsitelty laajemmin kuin oli ollut tarpeellista. Työntekijöiden ja soveltuvin osin myös työnhakijoiden henkilötietojen käsittelyyn sovelletaan tietosuoja-asetuksen lisäksi työelämän tietosuojalakia (*laki yksityisyyden suojasta työelämässä 759/2004*). Työelämän tietosuojalain tarpeellisuusperiaate rajoittaa henkilötietojen käsittelyä tiettyihin tilanteisiin. Tarpeellisuusperiaatteen mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.

Tapauksista voit lukea tarkemmin oheisesta pdf-tiedostosta.

PDF	Tapauksista voit lukea tarkemmin tästä.