

Asia: VN/23585/2023

Lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Lausunnonantajan lausunto

Mitkä ovat olleet yleisen tietosuoja-asetuksen soveltamiseen liittyvät merkittävimmät hyödyt ja haasteet?

Yleinen tietosuoja-asetus on merkittävästi lisännyt tietoisuutta ja ymmärrystä tietosuojasta. Euroopan laajuinen harmonisointi on helpottanut tietosuojatyötä. Nyt tunnistetaan yleisesti paremmin henkilötietojen käsittelytilanteita ja osataan paremmin ottaa huomioon henkilötietojen käsittelyyn liittyviä vaatimuksia.

Henkilötietojen suoja toteutuu paremmin kuin vanhan kansallisen henkilötietolain aikana. Nyt rekisterinpitäjä joutuu perehtymään siihen, mitä tietoja sillä on ja mitä tietoja se hallitsee. Myös tietojen säilytysajat on määritelty paremmin ja tarpeettomia tietoja on poistettu järjestelmällisemmin.

Keskeisin haaste on yleisen tietosuoja-asetuksen tulkinnanvaraisuus sekä valtava määrä Euroopan tietosuojaneuvoston (EDPB) ohjeistuksia.

Suomessa tietosuojavaltuutetun toimistosta on vaikea saada ohjeistusta tai neuvontaa. Myös viranomaispäätöksiä ei julkisteta johdonmukaisesti lukuun ottamatta sanktiopäätöksiä. Yritysten oikeusturvan kannalta olisi toivottavaa, että tietosuojavaltuutetun toimistosta annettaisiin kirjallisia ohjeita ja kannanottoja. Suomalaisille yrityksille on haastavaa seurata muissa EU-maissa kansallisilla kielillä annettuja päätöksiä. Tästä huolimatta kotimainen viranomainen on vedonnut näihin ratkaisuihin edellyttäen yksittäisen yrityksen tuntevan EU-laajuisesti eri kansallisten tietosuojaviranomaisten ratkaisuja.

Yleinen tietosuoja-asetus on lisännyt huomattavasti yritysten hallinnollista taakkaa ja aiheuttanut lisäkustannuksia. Voidaan perustellusti kysyä, onko tällainen kuormitus ollut tarkoituksenmukaista

ottaen huomioon henkilötietojen edellyttämä tosiasiallinen suojantarve. Nykyinen tietosuojalainsäädäntö on lähtökohdiltaan hyvin teoreettista, sisällöltään paikoin epäselvää ja käytännön toimintaan usein huonosti sovitettavissa olevaa.

Tietosuojavaatimusten harmonisointi ei ole ulottunut henkilötietojen käsittelyyn työsuhteen yhteydessä, mikä tuloksena jäsenvaltioiden välillä on edelleen eroja. Yleinen tietosuoja-asetus on lisännyt dokumentointivaatimuksia, mistä on aiheutunut lisäkustannuksia. Kansainvälisiin siirtoihin on liittynyt oikeudellista epävarmuutta ja sopimuksiin liittyviä vaatimuksia, joista on aiheutunut paljon hallinnollista taakkaa. Kansainvälisiin siirtoihin liittynyt lisätyö ei aina ole ollut järkevissä suhteissa siirtoihin liittyviin todellisiin riskeihin.

Tietojen käyttötarkoitusten kattava määrittely ennen käsittelyn aloittamista on aiheuttanut haasteita. Käyttötarkoitukset saattavat myös käsittelyn aikana muuttua tai laajentua. Kaikkia rekisteröityjä ei ole mahdollista tavoittaa helposti sähköisin menetelmin eivätkä kaikki tavoitetut reagoi pyydetyllä tavalla, vaan ovat välinpitämättömiä.

Eräät rekisteröidyt käyttävät oikeuksiaan shikaaninomaisesti väärin rekisterinpitäjää kohtaan esimerkiksi tekemällä erittäin laajoja tarkastuspyyntöjä. Usein rekisteröity ei ymmärrä oikeuksiaan tai sitä, mihin toimiin hän on antanut suostumuksen, mistä on sovittu ja minkälaisia oikeuksia ja velvollisuuksia rekisterinpitäjällä on muun muassa tietojen säilytyksen osalta. Usein rekisteröity ei lue tarjolla olevaa informaatiota.

Onko tietosuojalaki koettu yleisesti toimivaksi? Minkälaisia haasteita sen soveltamisessa on ilmennyt?

Pääsääntöisesti tietosuojalaki on ollut toimiva. Epäkohdaksi on koettu se ettei viranomainen ole ollut sanktioiden piirissä. Lisäksi vaikka Suomessa on kymmenen vuoden määräaika rikkomusten osalta, niin rangaistusluontoisia seuraamuksia voidaan määrätä tietosuoja-asiassa, jota ei katsota rikokseksi, paljon kauemmin.

Onko yleisen tietosuoja-asetuksen mahdollistamaa sääntelyliikkumavaraa käytetty EU:ssa ja Suomessa tarkoituksenmukaisella tavalla? Jos ei, miten ja minkälaisia tilanteita varten tietosuoja-asetuksen sääntelyliikkumavaraa tulisi käyttää eri tavoin kuin on tehty?

Suostumus-termiä on käytetty laissa yksityisyyden suojasta työelämässä tavalla, joka ei vaikuta täyttävän yleisen tietosuoja-asetuksen ja siihen liittyvien eurooppalaisten viranomaisohjeiden ehtoja suostumukselle. Tämä on aiheuttanut tulkintaongelmia. Suomen vanhat erityislait tulisivat käydä uudelleen läpi ja yksinkertaistaa tai poistaa mahdollisuuksien mukaan.

Millä toimialoilla yleistä tietosuoja-asetusta on pantu täytäntöön tehokkaasti ja onnistuneesti huomioiden asetukselle asetetut tavoitteet edistää rekisteröityjen oikeuksien ja vapauksien toteutumista sekä edistää tiedon vapaata liikkuvuutta EU-alueella?

-

Minkälaisia haasteita on ilmennyt yleisen tietosuoja-asetuksen ja kansallisen lainsäädännön tai muun EU-lainsäädännön yhteensovittamisessa eri soveltamistilanteissa?

Kysymyksissä, joissa on useita tai kaikkia EU-maita koskeva ulottuvuus, kansalliselta viranomaiselta ei ole saatu kannanottoa tai ohjeistusta. Myös sektorikohtaisen sääntelyn ja yleisen tietosuoja-asetuksen välisiin tulkintaristiriitoihin ei ole saatu kansalliselta viranomaiselta ohjeita tai neuvoja, mikä on valitettavaa.

Käsitys siitä, mikä on henkilötietoa, tuntuu olevan erittäin laaja ja siihen liittyy epävarmuuksia. Asiassa tulisi tunnustaa riskipohjaisuus, sillä jos esimerkiksi laitemittausdata voitaisiin tulkita henkilötiedoksi, mutta sitä käsittelee vain yksi tai muutama toimija, joilla ei ole tarvetta käyttää tietoa henkilöön liittyen, olisi tarkoituksenmukaista, että tilannetta ei tarkasteltaisi henkilötiedon käsittelynä.

Onko eri jäsenvaltioiden tietosuojalainsäädäntöjen eroavaisuuksiin ja täytäntöönpanoon liittyen tunnistettu haasteita? Jos on, minkälaisia haasteita?

On usein vaikea tietää mitä muissa maissa on tehty ja paikallisen sääntelyn mahdollisuus luo epävarmuutta, mistä syystä aina erikseen pyritään tarkastamaan, ettei kansallista poikkeusta kyseisessä maassa ole.

Ovatko Euroopan tietosuojaneuvoston antamat ohjeet auttaneet käytännön soveltamistilanteisiin liittyvien ratkaisujen tekemisessä? Mitä yleisen tietosuoja-asetuksen tulkintaa koskevia ohjeita vielä tarvittaisiin?

EDPB:n ohjeet ovat usein hyvin tulkinnanvaraisia ja niiden määrä on jo nyt liiallinen. Lisäksi ne ovat hyvin pitkiä ja teoreettisia, mikä vaikeuttaa niiden käyttöä yrityksissä. Ohjeet ylittävät asetuksen veloitteet usein venyttäen asetuksen tulkintaa, mikä ei ole kannatettavaa.

Ohjeet eivät myöskään aina toimi käytännössä, mikä heikentää niiden uskottavuutta ja vaikeuttavat tietosuoja-ammattilaisten työtä yrityksissä. Ohjeet eivät useinkaan helpota yleisen tietosuoja-asetuksen noudattamista, vaan lisäävät sen noudattamiseen liittyvää epävarmuutta.

Lisäksi ei ole selvää, ovatko ohjeet oikeasti ohjeita ja suosituksia vai sitovia sääntöjä, joiden rikkomisesta sanktiomahdollisuus.

Onko edustamanne organisaatio ollut mukana laatimassa yleisen tietosuoja-asetuksen 40 artiklan mukaisia käytännesääntöjä tai harkinnut niiden laatimista? Mitkä ovat käytännesääntöjen laatimiseen liittyviä merkittävimpiä hyötyjä ja haasteita?

Onko yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvä seuraamusjärjestelmä Suomessa tehokas ja tarkoituksenmukainen? Mitä merkittävimpiä hyötyjä ja haasteita seuraamusjärjestelmään liittyy?

Yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvässä seuraamusjärjestelmässä on ollut Suomessa toivomisen varaa. Viranomaisen toiminta on toistaiseksi ollut reaktiivista ja pohjautunut kanteluihin. Viranomaisen toiminta on ollut hidasta, mikä on ollut haasteellista tutkinnan kohteena olevan yrityksen näkökulmasta. Asioiden nopeammasta käsittelystä hyötyisi koko ala, sillä muut voisivat nopeammin sopeuttaa oman toimintansa oikeanlaiseksi.

Toivomme, että viranomaiset antaisi ensin ohjeita ja neuvoja ja vasta niiden noudattamisen laiminlyönnistä seuraisi sanktioita. Tämä olisi kaikkien osapuolien edun mukaista. Tällä hetkellä rekisterinpitäjä on voinut joutua tilanteeseen, jossa viranomaiset on todennut toimitun väärin, mutta viranomaiset ei ole antanut ohjeita tai neuvoja tilanteen korjaamiseksi oikealle tolalle ja kun myöhemmin asiaan on palattu ja korjausyrityksestä huolimatta viranomaiset on todennut, ettei veloitetta ole noudatettu, on määrätty sanktio.

Myös julkisen sektorin tulisi Suomessa olla sanktioiden piirissä.

Ovatko yleisen tietosuoja-asetuksen kansainväliset tiedonsiirtomekanismit toimivia vai tulisiko niitä kehittää edelleen ja miten niitä tulisi kehittää edelleen? Mitkä ovat olleet kansainvälisiin tiedonsiirtoihin liittyvät merkittävimmät hyödyt ja haasteet?

Kansainväliset tiedonsiirtomekanismit ovat työläitä ja niihin sisältyy paljon epävarmuutta, mistä syystä yritykset ovat jopa välttäneet kv. tiedonsiirtoja, mikä ei ole hyvä asia Suomen kilpailukyvyyn näkökulmasta. Myöskään monikansalliset yritykset eivät aina toimi tiedonsiirtomekanismien edellyttämällä tavalla. Tällöin suomalainen yritys on vaikeassa tilanteessa, sillä usein ei ole mahdollisuutta ostaa vastaavaa palvelua muualta kohtuulliseen hintaan. Esimerkiksi sopimuksesta huolimatta alihankkijasta ilmoittaminen ei useinkaan toimi asetuksen esittämällä tavalla.

Olemassa olevien sopimuskuppaneiden osalta tiedonsiirtomekanismien raskaus johtaa käytännössä liiketoiminnan haluttomuuteen selvittää koko alihankintaketjua, sillä koetaan hankalaksi tai jopa mahdottomaksi tehdä asiat täysin oikein ja toteuttaa kaikki siirtoihin liittyvät veloitteet.

EU:n ulkopuolisten maiden lainsäädännön seuraaminen vaatii suomalaiselta yritykseltä osaamista ja taloudellisia resursseja. Kun suomalainen yritys toimii rekisterinpitäjänä, se on viime kädessä vastuussa kv. siirron lainmukaisuudesta. Tällöin jää usein huomioimatta alihankkijoina toimivien teknologiajätien markkinavoima, sillä usein suomalaisella yrityksellä on vaihtoehtoina joko hyväksyä teknologiajätin palveluun kuuluvat siirrot sellaisenaan tai jättää mahdollisesti liiketoiminnan kannalta hyvinkin kriittinen palvelu hankkimatta. Esimerkiksi tietosuoja-asetuksen 28 artiklassa taattu rekisterinpitäjän mahdollisuus vastustaa alihankkijan käyttöä ei vaikuta asiaan, sillä

vastustusoikeus on useimmissa sopimuksissa toteutettu rekisterinpitäjän oikeutena lopettaa palvelun käyttö.

Komission tulisi tehdä enemmän adequacy-tutkimuksia ja -päätöksiä sen sijaan että yksittäisen yrityksen tulisi kyetä tekemään tapaus- tai maakohtaisia arvioita tietosuoja- ja vastaavan lainsäädännön tilasta ja sen vaatimista suojaustoimenpiteistä kolmansiin maihin tapahtuvissa tiedonsiirroissa. Olisi kohtuullista, että viranomaistaho antaisi selkeitä päätöksiä siitä, mitä ja millä edellytyksillä voi tehdä.

Onko yleisen tietosuoja-asetuksen ns. laajennettu alueellinen soveltamisala, joka kattaa myös EU:n markkinoilla toimivien kolmansien maiden toimijoiden suorittaman henkilötietojen käsittelyn, toiminut tarkoituksenmukaisella tavalla? Olisiko yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvää yhteistyötä kolmansien maiden kanssa tarpeen kehittää ja miten?

-

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

-

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

-

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

-

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Rekisterinpitäjä ja henkilötietojen käsittelijä

-

Kommentit yleisen tietosuoja-asetuksen V lukuun – Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille

-

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

-

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

-

Kommentit yleisen tietosuoja-asetuksen VIII lukuun – Oikeussuojakeinot, vastuu ja seuraamukset

-

Kommentit yleisen tietosuoja-asetuksen IX lukuun – Tietojenkäsittelyyn liittyviä erityistilanteita koskevat säännökset

-

Aalto-Setälä Minna
Keskuskauppakamari