

Oikeusministeriölle

Suomen Perimistöimistöjen Liitto ry:n vastaus oikeusministeriön lausuntopyyntöön VN/5281/2019: Yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Mitkä ovat olleet yleisen tietosuoja-asetuksen merkittävimpiä hyötyjä?

Tietosuojan merkityksen korostuminen ja siihen panostaminen yrityksissä on johtanut myös monien tarpeellisten kehityskohteiden löytämiseen ja menettelytapojen yhtenäistämiseen ja selkiyttämiseen.

- Rekisteröityjen oikeudet parantuneet
- Euroopassa yhtenäinen lainsäädäntö
- Läpinäkyvyys missä tietoja käsitellään
- Tietosuojaan suhtaudutaan vakavammin

Mitkä ovat olleet yleisen tietosuoja-asetuksen soveltamisessa ja toimivuudessa suurimpia haasteita?

Soveltamiseen liittyvät tulkintaepäselvyydet. Yhtenäisen tulkinta- ja ratkaisukäytännön puuttuminen ja siihen liittyvät haasteet tulevat olemaan ongelma myös tulevaisuudessa johtuen jäsenmaiden erilaisesta lainsäädäntötaustasta ja kulttuureista.

- oikeustapausten ja viranomaislinjausten puuttuminen
- WP 29 antamien tietosuojadirektiivin aikaisten tulkintaohjeiden ja lausuntojen ajantasaisuus ja sovellettavuus GDPR:n voimaantulon jälkeen.
- Asetuksen vaikeaselkoisuus ja suuri viittausten määrä

Tietosuoja-asetusta on voitu tulkita eri jäsenvaltioissa eri tavalla rekisterinpitäjän ja henkilötietojen käsittelijän roolien osalta. Jos on ollut erilainen näkemys tietosuoja-asetuksen mukaisista em. rooleista, niin on kulunut normaalia enemmän aikaa esimerkiksi henkilötietojen käsittelysopimusten laatimiseen ennen kuin on päästy molempia osapuolia tyydyttävään ratkaisuun sopimusehtojen osalta.

Kun tietosuojavastaavan tehtävät on ulkoistettu niin tietosuojapalveluita tarjoava taho ei ole välttämättä sisäistänyt asiakkaansa tietosuojaprosesseja niin syvällisesti kuin asiakas itse ja siten esimerkiksi henkilötietojen käsittelysopimuksen laadinta on ollut hitaampi prosessina em. tilanteessa henkilötietojen käsittelijän kuten esimerkiksi uuden alihankkijan kanssa.

Onko yleisen tietosuoja-asetuksen mahdollistamaa sääntelyliikkumavaraa käytetty Suomessa tarkoituksenmukaisella tavalla?

Ei kaikilta osin. Se, että hallinnollista seuraamusmaksua ei tietosuojalain mukaan Suomessa voida määrätä julkisyhteisöille luo epätasa-arvoisen asetelman eri toimijoiden välille ja voi johtaa jopa erilaisiin toimintatapoihin ja tulkintakäytäntöihin, kun yksityiset toimijat joutuvat toiminnassaan ottamaan huomioon hallinnollisen seuraamusmaksun riskin.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

-

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Käsittelyperusteiden tulkinnassa ja yhtenäisessä käytännössä oikean käsittelyperusteen valinnan osalta on edelleen huomattavaa vaihtelua sekä eri maiden ja toimijoiden kesken.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Viranomaisohjeistus sen suhteen millaista tunnistautumista rekisteröidyltä voidaan vaatia puuttuu ja käytännöt vaihtelevat.

Katsomme, että rekisterinpitäjällä tulee harjoitetun toiminnan ja tallennettujen tietojen luonteesta ja määrästä riippuen olla mahdollisuus vaatia rekisteröidyltä vahvaa tunnistautumista ennen tietojen luovuttamista. Näin sen vuoksi, että kyseessä saattavat olla laajamittaisetkin esimerkiksi henkilön taloudellista asemaa koskevat tiedot, jotka ovat rinnastettavissa arkaluontoisiin tietoihin.

Automaattisen päätöksenteon ja profiloinnin merkityssisällöt, erot ja suhde toisiinsa ovat osoittautuneet vaikeaksi hahmottaa.

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

DPA sopimusten raskaus ja sakon vyöryttäminen

Henkilötietojen käsittelyä koskevat sopimukset ovat usein pitkiä ja yksityiskohtaisia, verrattuna tietosuoja-asetuksen 28 artiklassa oleviin vaatimuksiin. Yhtenä taustasyynä sopimusten raskauteen lienee rekisterinpitäjien ja käsittelijöiden epätietoisuus siitä, millä tarkkuudella tällainen sopimus on tehtävä ja missä määrin poikkeukselliset tai jopa teoreettiset käsittelytilanteet tulee kattaa (esim. Infrastructure as a Service -palveluntarjoajien kohdalla). Toisena taustasyynä saattaa olla taipumus ylivarovaisuuteen. Joka tapauksessa sopimusten raskaus merkitsee sopimusneuvottelujen keston pitkittymistä ja kustannusten kasvua.

Etenkin kooltaan suuremmat rekisterinpitäjät ovat taipuvaisia kohdistamaan varsin raskaita tietosuojavelvoitteita henkilötiedon käsittelijöinä toimivia alihankkijoitaan kohtaan. Esimerkkinä voidaan mainita erittäin lyhyt aika ilmoittaa

tietosuojaloukkauksesta. Myös suoranaisia ylilyönnejä vaatimusten ankaruudessa on esiintynyt, joista esimerkkinä mainittakoon koko alihankintaketjun käsittävän listan toimittaminen niistä henkilöistä, jotka käsittelevät sellaisia henkilötietoja, joiden rekisterinpitäjä kyseisen vaatimuksen esittäjä on. Vaikka käsittelijä itse pystyisikin vaatimukseen suostumaan, käsittelijän omien alihankkijoiden sitouttaminen vastaaviin vaatimuksiin voi osoittautua käytännössä mahdottomaksi. Hankaluuksia aiheutuu myös tilanteessa, jossa käsittelijä joutuu sovittamaan yhteen eri asiakkaidensa (rekisterinpitäjien) erilaisia vaatimuksia.

Edellä kuvattu kehityskulku hankaloittaa pienempien ja neuvotteluvoimaltaan heikompien yritysten mahdollisuutta toimia markkinoilla.

Lisäksi varsinkin kooltaan suuremmat yritykset pyrkivät - sinänsä ymmärrettävästi - varmistamaan sopimusteitse, etteivät hallinnolliset maksuseuraamukset jää niiden itsensä tappioksi, vaan ne kanavoituvat regressityyppisten sopimusklauusulien avulla pienempien sopimuskumppaneiden maksettavaksi. Sopimusoikeudellisesti ilmiö ei liene uusi, mutta hallinnollinen maksuseuraamus saattaa tällaisen käytännön vallitessa päätyä sellaisen tahon maksettavaksi, jota viranomainen ei seuraamusta määrätessään tarkoittanut. Tasavertaisten sopijapuolien kesken käytetään herkemmin ehtoja, joissa hallinnolliset maksuseuraamukset jäävät sen osapuolen maksettavaksi, jolle viranomainen on sen langettanut.

Tietojen käsittelyä koskevien sopimusten standardoiminen, mahdollisuuksien rajoissa, olisi toivottavaa.

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

Tietojen siirto pilvipalveluihin

Yritykset voivat saavuttaa tehokkuus- ja kustannushyötyjä hyödyntämällä pilvipalveluja, mutta niiden käyttöönottoa hidastaa epäselvyys siitä, missä määrin ja millaisin reunaehdoin tietosuoja-asetus sallii sellaisten palveluntarjoajien käytön, joiden pilvipalvelu sijaitsee EU:n ulkopuolella. Sama epäselvyys koskee myös sellaisia palveluntarjoajia, joiden pilvipalvelu toteutetaan Euroopassa, mutta joihin EU:n ulkopuolisten valtioiden viranomaiset saattavat kohdistaa tietojen luovuttamista koskevia vaatimuksia. Viimeksi mainitusta tilanteesta käynee esimerkkinä USA:n CLOUD Act.

Osa rekisterinpitäjistä on toisaalta valinnut linjan, jonka mukaan he eivät hyväksy henkilötietojen siirtoa EU:n ulkopuolelle lainkaan.

Edellä kuvattu epätietoisuus ja varovaisuus antavat kilpailuetua täysin eurooppalaisille ja Euroopassa toimiville palveluntarjoajille, mutta lisäävät toisaalta rekisterinpitäjien ja käsittelijöiden kustannuksia. Tietävästi on myös sellaisia kansainvälisten suuryritysten tarjoamia tiedonhallinta- ja käsittelypalveluja, joita eurooppalaisilta palveluntarjoajilta ei edes saa.

Kommentit yleisen tietosuojasetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Suomen tietosuojavaltuutetun nykyinen tietosuojaloukkausten ilmoitusprosessi lomakkeineen on vielä kankea ja sen kehittäminen olisi toivottavaa. Erityisesti ilmoituksen myöhempi täydentäminen on hankalaa.

Tarkennukset olisivat toivottavia TSV:n sivuilla esitettyihin tietosuojatyöryhmän esimerkkitilanteisiin, joiden tarkoituksena on auttaa rekisterinpitäjiä määrittämään, onko niiden tehtävä ilmoitus erilaisissa henkilötietojen tietoturvaloukkaustilanteissa.

Kommentit yleisen tietosuojasetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

Tietosuojakäytänteiden erot eri maissa

Yhtenäiset tulkintasuositukset ja yhtenäinen ratkaisukäytäntö kansallisten valvontaviranomaisten välillä puuttuvat vielä. Pohjoismaisten tietosuojaviranomaisten käynnistämä yhteistyö on tästä hieno esimerkki, mutta se ei ole juuri vielä tuonut käytännössä näkyvyyttä tai tuloksia.

Eri maiden tietosuojakäytänteet eivät ole tietosuojasetuksesta huolimatta samanlaisia, mihin rekisterinpitäjät ja käsittelijät saattavat törmätä sopimuksia laadittaessa. Useammassa maassa toimivat yritykset saattavat käyttää sopimuksissaan ehtoja, joilla sinällään pyritään toteuttamaan tietosuojaa, mutta jotka heijastavat yrityksen kotipaikan käytänteitä ja sopivat toisen maan lainsäädäntöön huonosti. Henkilötiedon käsittelijöille on esimerkiksi saatettu esittää sopimusehtoja, joiden mukaan henkilötietoon käsiksi pääsevien työntekijöiden rikostaustat tulee selvittää ja tiettyjen kriteerien täytyessä pääsy henkilötietoon estää. Vaikka tällainen menettely saattaa olla hyväksyttävää rekisterinpitäjän kotimaassa, se voi olla ongelmallista muualla, kuten Suomessa. Riskinä on, että asiakassuhteen vaalimiseksi kyseenalaisiinkin vaatimukseen kuitenkin suostutaan.

Kommentit yleisen tietosuojasetuksen VIII lukuun – Oikeussuojakeinot, vastuu ja seuraamukset

Ei kaikilta osin. Se, että hallinnollista seuraamusmaksua ei tietosuojalain mukaan Suomessa voida määrätä julkisyhteisöille luo epätasa-arvoisen asetelman eri toimijoiden välille ja voi johtaa jopa erilaisiin toimintatapoihin ja tulkintakäytäntöihin, kun yksityiset toimijat joutuvat toiminnassaan ottamaan huomioon hallinnollisen seuraamusmaksun riskin.

Helsingissä 17. päivänä syyskuuta 2019

Suomen perimistöimistöjen Liitto ry

Hallitus