Valtori

Lausunto

06.09.2023 Valtori/2256/00 05 00/2023-1

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?

Hyödyt

- Tietosuojatyö on yhtenäistynyt.
- GDPR on parantanut rekisteröityjen oikeuksia ja niiden toteutumista ihan kaikessa toiminnassa.
- GDPR toimii kannusteena parantaa tietoturvan tasoa palveluissa.
- Uudet ohjelmistot ovat kehittyneet rekisteröidyn oikeuksia huomioivaan suuntaan

Haasteet

- GDPR:n fokus näyttää kohdistuvan kaupallisten toimijoitten henkilötietojen käsittelyyn. Näin ollen valtion hallinnossa tapahtuva henkilötietojen käsittely on jäänyt vähemmälle ohjaukselle.
- Lainsäädäntöjen yhteensovittaminen on haastavaa, kuten esimerkiksi laki sähköisen viestinnän palveluista, julkisuuslaki, laki yksityisyyden suojasta työelämässä sekä vaikka ääriesimerkkinä Yhdysvaltain tiedustelulaki.
- Uudet vaikutustenarvioinnin (DPIA ja TIA) velvoitteet vaativat osaamista ja resursseja. Esimerkiksi TIA:ssa pitää arvioida kolmannen valtion lainsäädäntöä ja viranomaistoimintaa, mikä on kohtuuton vaatimus monessa organisaatiossa.
- --> Voisiko tätä jotenkin yhtenäistää, että valtio-arvioita olisi tehty keskitetysti?

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

- Soveltamisen haasteena on se, että laissa on paljon vaatimuksia, mutta siinä ei juurikaan kuvata kontrolleja, joilla vaatimuksia toteutetaan. Organisaation pitäisi itse arvioida, mikä on riittävä kontrolli. Tähän olisi hyvä saada joko säädösparannus tai lisää viranomaisohjausta.

- Nykytila tarjoaa mahdollisuuden ristiriitaiselle tulkinnalle, kun eri lakien roolit, oikeudet ja velvoitteet menevät ristiin. Esimerkkinä GDPR ja laki sähköisen viestinnän palveluista.

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?

- Kansallista liikkumavaraa kannattaa käyttää siten, että kansallisesti ei tiukenneta EU-säädöksiä.

- Tähän saakka esimerkiksi hallinnollisia sakkoja ei ole säädetty kansallisesti noudatettavaksi julkiselle sektorille, mikä on ollut hyvä. Alla on perusteluja:

-> Rahan siirtäminen valtion taskusta toiseen ei ole oikea tapa rankaista virastojen ja muun julkishallinnon lainsäädännön noudattamista.

-> Julkishallinnon pitäisi varautua keräämällä sakkokassa asiakkailta/ valtion rahoituksesta, mikä poistaa valtion varoja käytöstä pysyväissäilytykseen.

-> Julkishallinto noudattaa muitakin lakeja viran puolesta ja niiden noudattamatta jättämisellä voi olla monenlaisia seurauksia niin lain rikkojalle, kuin organisaatiollekin

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?

- Tulli ja Verohallinto ovat mm. olleet edelläkävijöitä. Niiden hyviä käytäntöjä olisi hyvä saada koulutusten ja oppaiden muodossa levitettyä.

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

- Haasteita löytyy. Eri lakeja valvovat viranomaiset voisivat antaa rajatapauksista lisää tulkintaohjeita (Esim Traficom ja TSV yhteisistä rajapinnoistaan)

- Laki sähköisen viestinnän palveluista on vaikea yhteensovittaa tietosuoja-asetuksen kanssa. Tähän olemme saaneet Traficomilta ohjausta heidän toimivaltansa osalta, mutta tarvitsisimme lisäksi Tietosuojavaltuutetun toimiston ohjausta, jotta voisimme ratkaista rajatapauksia.

- GDPR ja Julkisuuslain yhteensovittamisen ongelmat: Julkisuuslain mukaisten tietopyyntöjen osalta tulisi arvioida samalla henkilötietojen käsittely. Tämän muistaminen voi olla vaikeaa, kun asian käsittelijä ei ole tietosuoja-asiantuntija.

- GDPR mukaisissa vaikutustenarvioinnissa (DPIA) tulisi tehdä myös arviointi rooleista sähköisen viestinnän palvelulain mukaisesti, mutta tähän ei ohjeisteta, koska tietosuojavaltuutettu ja Traficom eivät anna yhteisiä ohjeita.

- On epäselvää, milloin rekisteröityjä tulisi informoida palveluiden käytössä sellaisessa tilanteessa, jossa sekä laki sähköisen viestinnän palveluista että tietosuoja-asetus säätävät informoinnista.

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

- Hyvinä esimerkkeinä aktiivisesta ja keskitetystä tietosuojatyöstä voimme nostaa Ranskan ja Alankomaiden tietosuojaviranomaiset.

- Suomessa on tietosuojan osaamis- ja resurssipula.

- Tietosuojalainsäädäntöjen eroavaisuuksiin emme ole törmänneet lainkaan, koska kansallinen liikkumavara on suht vähäinen.

- Suomesta puuttuvat kansalliset tietosuojan sertifikaatit, jollaisia esim. Ranska ja Belgia ovat tehneet. Tällaista toimintaa voisi tehdä esim. pohjoismaisena yhteistyönä.

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

- Tiedonsiirto EU:n ulkopuolelle: Schrems II päätöksen jälkeen saadut ohjeet TIA:n tekemiselle sekä EDPB Guidelines 1/2020 ovat olleet arvokkaita.

- Rekisterinpitäjän ja käsittelijän rooleja koskevat ohjeet ovat auttaneet linjaamaan rooleja rajanvetotilanteissa, joissa olemme pohtineet mm. yhteisrekisterinpitäjyyttä (EDPB Guidelines 7/2020).

- Suurin osa ohjeista on kuitenkin kohdennettu yksityiselle sektorille.

- Toivoisimme lisää julkishallinnolle ja palvelukeskuksille kohdennettuja ohjeita.

- Ohjeet (guidelines) ovat usein hyvin abstraktilla tasolla, eli käyttötapaukset puuttuvat.

- Joissain aiemmissa käännöksissä on ollut ongelmia.

- EDPB:n ohjeiden tulkinta-avuksi kaipaisimme lisäksi kansallisia koulutuksia ja käytännönläheistä ohjeistusta tietosuojavaltuutetun toimistosta.

- Tällä hetkellä tietosuojavaltuutettu ja EDPB ovat antaneet tiukan tulkinnan mukaisia ohjeita monessa asiassa ja toivoisimme enemmän riskiperusteista pohdintamahdollisuutta. Käytännön esimerkki tiukan tulkinnan seurauksista: Jos tulkitsisimme GDPR:ää kirjaimellisesti, kuten TSV on tehnyt, että IP-osoite on yksilöivä henkilötieto, se tarkoittaisi sitä, että internetin GDPR:n mukainen käyttö on mahdotonta. --> Jos palvelusta välittyy ainoana tietona IP-osoite, voitaisiinko tällöin

arvioida riskiperusteisesti haittoja rekisteröidyn oikeuksille ja vapauksille? Toinen tiukan linjan tulkinta on tiedon siirrossa ETA-alueen ulkopuolelle. Voisiko siinä punnita riskejä kyllä/ei-linjausten sijasta?

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?

- Valtori on ollut mukana Cirrus-hankkeessa, jossa pyritään neuvottelemaan muutaman toimittajan kanssa kansallisista pilvipalveluvaatimuksista

- Valtori on vapaamuotoisemmin tehneet yhteistyötä Valtorin asiakkaiden kanssa tietosuojan kypsyystason parantamiseksi.

- Valtori on tehnyt yhteistyötä Tiedonhallintalautakunnan kanssa Julkri-vaatimusten hankintatyökalun kehittämiseksi, mikä on sisältänyt tietosuojaosion

- Valtori on tehnyt vapaamuotoisemmin yhteistyötä VAHTI organisaation tietosuojan kehittämisen työryhmän kanssa tietosuojaliite mallin julkaisemiseksi sekä kansallisten tietosuojaan liittyvien ohjeiden ja koulutusten julkaisemiseksi. Valtori on lisäksi jakanut hyviä käytäntöjä ja malleja VAHTI verkostossa.

- Käytännesäännöt kannattaa tehdä yhteistyössä muiden organisaatioiden kanssa ja julkaista esim. VAHTI tai muussa yhteistyössä, jotta mahdollisimman moni pääsee niihin käsiksi.

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

- Tähän saakka esimerkiksi hallinnollisia sakkoja ei ole säädetty kansallisesti noudatettavaksi julkiselle sektorille, mikä on ollut hyvä. Alla on perusteluja:

-> Rahan siirtäminen valtion taskusta toiseen ei ole oikea tapa rankaista virastojen lainsäädännön noudattamista.

-> Julkishallinnon organisaatioiden pitäisi varautua keräämällä sakkokassa asiakkailta/ valtion rahoituksesta, mikä poistaa valtion varoja käytöstä pysyväissäilytykseen.

-> Julkishallinto noudattaa kaikkia muitakin lakeja viran puolesta ja niiden noudattamatta jättämisellä voi olla monenlaisia seurauksia niin lain rikkojalle, kuin organisaatiollekin.

- Täytäntöönpanon kehittämisessä painotuksen tulisi rankaisun sijaan olla ennaltaehkäisyssä ja ohjeistuksessa. Esimerkiksi TSV:n lausuntomenettely on olennaisessa roolissa ennaltaehkäisemässä ongelmia, joten siihen toivoisimme kehityspanostusta ja resursseja myös dialogiin organisaatioiden kanssa.

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?

- Painotus tulisi kansainvälisessä tiedonsiirrossa siirtyä riskiperusteiseen arviointiin ehdottomien kyllä/ei-linjausten sijasta. Tähän toivoisimme ohjausta valvovalta viranomaiselta.

- Uudet vaikutustenarvioinnin (DPIA ja TIA) velvoitteet vaativat osaamista ja resursseja. Esimerkiksi TIA:ssa pitää arvioida kolmannen valtion lainsäädäntöä ja viranomaistoimintaa, mikä on kohtuuton vaatimus monelle organisaatiolle

- Voisiko TIA-valtioarviointien tekemistä jotenkin yhtenäistää edes julkishallinnossa, että valtio-arvioita olisi tehty keskitetysti a) virkatyönä tai b) kilpailuttamalla listan toteuttaja ja ylläpitäjä?

- Tietosuojavaltuutetun DPIA-työkalua voisi kehittää eteenpäin säännöllisesti, eli lisätä ja parantaa sitä palautteen avulla. Koska TSV:n resurssit ovat rajalliset, palautteen keräämiseen ja työkalujen kansalliseen kehittämiseen voisi pyytää avuksi esim. Kuntaliittoa ja VAHTI työryhmää.

o Suosittelemme tutustumaan Hankinta Suomi ja HankintaKeino -verkostoihin, jotka ovat tuoneet eri tahoja yhteen saman teeman ympärille ja ne ovat saaneet paljon aikaan.

o Voisimme tehdä jotain samanlaista tietosuojan kanssa, eli ensin hankkeistaa kehitystyö EU-rahoituksella ja myöhemmin vakinaistaa se osaksi jonkun/joidenkin organisaatioiden perustehtäväksi.

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?

- Jos tällä tarkoitetaan EU-komission riittävyyspäätöksiä, niin ne ovat olleet selkeitä ja hyviä. Lisäksi komission valtio-arvioinnit ovat olleet suureksi avuksi, kun olemme tehneet omia Transfer Impact Assessment arvioita tiedon siirrosta ETA-alueen ulkopuolelle.

- Olemme huolissamme, kuinka kestävällä pohjalla on komission päätös hyväksyä EU-USA tietosuojakehys (vrt. EU-parlamentin päätöslauselma 11.5.2023, jossa nostetaan riskejä https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_FI.html)

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

-

Kynkäänniemi Päivi
Valtori - Valtorin tietosuojatiimi ja lakipalvelut yhteistyössä