Asiakkuusmarkkinointiliitto ry

Lausunto

06.09.2023

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?

Henkilötietoja koskevan käsittelyn merkitys ja siihen liittyvät toiminnalliset osa-alueet ovat GDPR:n myötä kokonaisuutena saaneet ansaitsemaansa huomiota. Henkilötietojen käsittelyyn ja yksityisyyden suojaan liittyvä suunnittelun, dokumentoinnin ja tekemisen taso, laajuus ja syvyys sekä läpinäkyvyys on kasvanut. Rekisteröityjen asema on vahvistunut.

Sääntelyn vaikeatulkintaisuus, epäselvyys ja joustamattomuus koetaan yleisesti haasteeksi eri sektoreilla. Viranomaisten ohjaus- ja neuvontatoiminnan ei koeta riittävästi ja joustavasti tukevan rekisterinpitäjien tai käsittelijöiden tietosuojatyötä. Oikeusvarmuuden puute nousee jatkuvasti esiin.

Valvovien viranomaisten toiminta kokonaisuudessaan liian vahvasti sanktio- ja rajoitekulttuurin sävyttämää. Sääntelyn kokonaisuus ei ole tasapainoinen, esimerkkinä evästesääntelyn muuta sääntelyä pidemmälle ja tiukemmalle viedyt linjaukset ja tulkinnat. Tilannetta ei yksittäisenä elementtinä helpota GDPR:n heikko ja osin virheellinen suomenkielinen versio, esimerkiksi eräitä velvoitesäännöksiä muihin kieliversioihin verrattuna tiukentaen.

Erityisen suuri haaste on viranomaisten puutteellinen ymmärrys henkilötietojen käsittelyn tyyppitilanteiden luonteesta, joka on pääosin ryhmä- ja yleisötasoinen. Yksittäinen henkilötieto on käytännössä usein raaka-aine hyödylliseen raportointiin, asiakaspalveluun, palvelukehitykseen, palvelutarjontaan, sopimuksen täytäntöönpanoon ja muihin niin rekisteröityjä kuin rekisterinpitäjiä hyödyttäviin tarkoituksiin yhteiskunnan kaikilla sektoreilla. Tässä kontekstissa yksittäiseen tietoon tai rekisteröityyn liiaksi tai jopa virheellisesti pureutuva näkökulma aiheuttaa usein vinoumaa tulkinnoissa ja johtopäätöksissä.

Eurooppalaisessa tietosuojan sääntelykulttuurissa henkilötietojen perusteltu, suunniteltu ja informoitu käsittelykin nähdään aivan liian usein yksityisyyden suojaan puuttumisena tai sen loukkauksena vaikka pääosin on kyse modernin asiakaslähtöisen tai palvelullisen toiminnan massaluonteisista, tavanomaisista ja turvallisista perusprosesseista sekä samalla globaalin kilpailukyvyn ylläpidosta ja kehittämisestä. Tähän liittyy kiinteästi esimerkiksi anonymisointi/pseudonymisointi -dynamiikka, johon liittyviä elementtejä on säädelty ja tulkittu liian ahtaasti – riskipohjaisella lähestymistavalla päästäisiin tässäkin kaikkia osapuolia paremmin hyödyttävään lopputulokseen. Kaikkeen toimintaan, myös henkilötietojen käsittelytoimintaan liittyvä toiminnan ja käyttötarkoituksien luonnollinen muuttaminen tulisi olla nykyistä joustavampaa.

Informointivelvoitteet laajenevat uusien linjausten, oikeustapausten ja erityislainsäädännön myötä tavalla, joka johtaa käytännössä information fatigue -tyyppiseen epätyydyttävään tilanteeseen. Mainittakoon lisäksi rekisteröityjen oikeuksien välineellinen väärinkäyttö, johon puuttumiseen ei voimassa oleva sääntely anna käytännössä juurikaan eväitä rekisterinpitäjille.

EDPB:n ohjaustoiminnan laatu on jatkunut yllättävänkin heikkona. Aivan liian pitkiä ohjeistuksia sisältäen säädöksiin perustumattomia kasuistisia tai käytännöstä vieraita ylitulkintoja, jotka osaltaan nakertavat viranomaistoiminnan legitimiteettiä. Normihierarkiassa hyvin alhaalla olevien EDPB-ohjeistusten sisältö kertautuu copy paste -tyyppisesti sellaisenaan viranomaisratkaisuihin ja jopa lakiesitysten perusteluteksteihin ilman tarkempaa tilanne- tai oikeudellista analyysiä tavalla, jota ei voida millään tavoin pitää asianmukaisena kehityskulkuna.

Tietosuoja-asetuksen tärkeisiin ydinperiaatteisiin perustuva riskiperustainen, tilanne- ja konktekstipohjainen lähestymistapa ei toteudu tällä hetkellä riittävällä tavalla. Tämä pääperiaate tulisi huomioida nykyistä paljon paremmin kaikessa viranomais- ja säädöstyössä. EU:n tietosuosääntelyn kokonaisuus rapauttaa tällä hetkellä kilpailukyvyn kannalta haitallisella tavalla asiakasymmärryksen kerryttämistä sekä sen jalkauttamista erityisesti online-ympäristössä. Asiakas, sopimus, asiakaskokemus ja asiakasymmärrys on jäänyt kokonaisuudessa hämmentävällä tavalla katveeseen.

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

Tietosuojalain soveltamiseen liittyy edellä 1-kohdassa kuvattuja yleishaasteita. Tietosuojalain suppeamman soveltamisalan vuoksi siitä spesifisesti kumpuavia haasteita on vähemmän. Esimerkkinä näistä mainittakoon tarve laajentaa 6 §:n 1-kohdan sanamuodon laajentaminen kattamaan haetun vakuutussuojan kohteena olevat henkilöt.

Julkisen sektorin oleminen fiskaalisten sanktioiden ulottumattomissa ei ole ollut tasapainoinen ratkaisu. Uusin hallitusohjelma lupaa tosin tähän muutosta.

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?

Tietosuoja-asetuksen sääntelyn ja valvonnan toimivuuden mukaan lukien sääntelyn liikkumavaran käytön aito kansallinen, konkreettinen seuranta on käytännössä ollut melko lailla ns. kuollut kirjain. Henkilötietojen käsittelyn sääntelykokonaisuuteen kuuluva työelämän tietosuojasääntely kaipaa modernisointia, joka jäi edellisellä hallituskaudella harmillisesti kesken.

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?

Kaiken, myös uuden ja valmisteilla olevan erityissääntelyn yhteensopivuus yleiseen tietosuojasääntelyyn tulisi varmistaa nykyistä paremmin. Nykytilanteessa esimerkiksi PSD2, ePrivacy/SVPL-sääntely, pankkisalaisuus- ja vakuutussalaisuussääntely ja työelämän tietosuojasääntely tulkintatraditioineen eivät ole tarkoituksenmukaisella tavalla yhteensopivia ja synkronoituja yleiseen tietosuojasääntelyyn nähden. Sektori- ja yleislainsäädännön välisiin hankaliin tulkintatilanteisiin on kovin hankala saada viranomaistukea, samoin kansainvälisen toimintaan liittyen.

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

Sekä säädös-, ohjeistus- että tulkintatasolla on käytännössä monenlaisia eroavaisuuksia eri EU-maiden välillä mikä hankaloittaa ja rasittaa useassa maassa toimivia rekisterinpitäjiä. On syytä nostaa erityisesti esiin erilaiset kriteerit liittyen tietoturvaloukkausilmoitusten tekemiseen eri maissa. Suomessa on liian alhainen kynnys sekä laadultaan puutteellinen viranomaisprosessi tältä osin.

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

Viittaamme tämän osalta 1-kohdassa lausuttuun. EDPB:n ohjeet eivät nykyisenkaltaisessa jatkumossa ole tkovin oimiva elementti sisällöllisesti eikä rakenteellisesti. On lisäksi syytä nostaa esiin EDPB:n ohjeistuksen kuulemisprosessi, jota useat tahot pitävät muodollisena välivaiheena ilman tosiallista mahdollisuutta vaikuttamiseen tai vuoropuheluun. 1-kohdassa mainittu riskiperustaisuuden puute on selkeä puute EDPB:n ohjeistuksissa ja toiminnassa muutoinkin. Usein on myös esitetty kysymys kuka valvoo EDPB:n ohjeiden säädöksiä ylittäviä tulkintoja ja puuttuu niihin?

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?

Sekä kansallisesti että EU-tasolla käytännesääntöjen tekeminen on koettu usein turhaksi ja liian työlääksi, erityisesti koska niissä hyödynnettävissä oleva riskiperustainen lähestymistapa ja mukanaan tuoma tilannekohtainen joustavuus on valitettavasti operatiivisesti rapautunut kasuististen ohjeistusten, oikeustapausten, tulkintojen ja ylitulkintojen vuoksi.

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

Tämän osalta nousee erittäin vahvasti viranomaisohjauksen ja neuvonnan puute. Viranomainen saattaa todeta lähes perustelematta ja ilman aiempaa huomautusta tai puuttumista jonkun toimintamallin vääräksi mutta ei prosessinkaan aikana ei anna rekisterinpitäjille riittävää ohjausta näiden sitä pyytäessä.

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?

Kansainväliin tiedonsiirtoihin liittyvä monimutkaisuus, mekanismit ja rasitteet liittyen esimerkiksi lainsäädäntötilanteen maakohtaiseen arviointiin tai tarvittaviin lisäsuojatoimenpiteisiin on liiaksi jätetty yksittäisten rekisterinpitäjien harteille tavalla, jota ei millään tavoin voi pitää tarkoituksenmukaisena tai tavoiteltavana. Tähän tarvitaan pitkäkestoisia, instituutiotasoisia ratkaisuja ja rakenteita, joissa otetaan myös huomioon teknologia-alan isojen palveluntarjoajien ylivertainen asema ja neuvotteluposition suhteessa kansallisiin rekisterinpitäjiin.

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

Anonymisoinnin ja pseudonymisoinnin nykymääritelmät ja -tulkinnat eivät palvele asetuksen tavoitteiden toteutumista. Henkilötiedon määritelmää lavennetaan liiaksi ottaen huomion eri käsittelytyyppien massa- ja yleisöluonteen. Terveyttä koskevan tiedon määritelmä ja tulkinnat laajenevat ja tiukkenevat jatkuvasti tavalla, joka ei palvele alkuperäistä tarkoitusta ja estävät hyötypalveluiden tarjontaa rekisteröidyille. Koko arkaluonteisten tietojen kategoria tulisi riskiperusteisesti arvioida uudelleen. Joint controller-tulkinnat eivät ole olleet tasapainoisia. Rekisterinipitäjä/käsittelijä – käsitteiden perustoimivuutta toimivuutta tulisi tarkastella eri tyyppitilanteita ja markkinakäytäntöä vasten.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Minimiperiaate on GDPR 5 artiklassa faktisesti tarpeellisuusperiaatteelle alisteinen. Tämän artiklan virheellinen vahvasti minimi-vetoinen tulkinta ja siihen liittyvät linjaukset, ohjeistukset ja kannanotot hankaloittavat tosiasiallisesti dataintensiivisen toiminnan aloittamista, harjoittamista ja kehittämistä. Katso myös 12-kohdan vastaus.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Tavanomainen, harmiton automaattinen prosessityö ja päätöksenteko on tarpeettomasti vaikeutunut. Siirrettävyys ei ole osoittautunut toimivaksi eikä tarpeelliseksi oikeudeksi. Rekisteröidyn oikeuksiin kytkeytyvä ”jäljennös”- ja ”kaikki” -rakenne ja velvoitemallit eivät ole toimivia kokonaisvaltaisen digitaalisuuden aikakaudella. Oikeutetun edun tavanomaiset perustellut tyyppitilanteet pitäisi saattaa tasapainotestin vaatimuksen ulkopuolelle (vrt UK:n tietosuojauudistus).

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

Tarvitaanko modernissa toiminnassa vielä erillistä selostetta käsittelytoimista? Onko tietoturvaloukkauksiin liittyvät nykyiset aikarajat ja vaatimukset asianmukaisia ja perusteltuja? Entä viranomaisten omien prosessien laatu tältä osin? Jos ja kun käsittelijä eräissä tapauksissa on tosiasiallisesti ainoa velvoitteen toteuttaja ja toteuttamisen tavan määrittäjä niin onko rekisterinpitäjä/käsittelijä-suhteen velvoitteet tasapainoisia, ottaen toisaalta huomioon mikroyrittäjyyden lisääntymisen käsittelijäpuolella ja toisaalta isot teknologia-alan palveluntarjoajat? Ovatko yhteisrekisterinpitäjyyden tulkinnat ajautuneet GDPR:n tavoitteiden ja käytännön järkevyyden ulkopuolelle?

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

Katso 10-kohdan vastaus.

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Katso 1-kohdan vastaus.

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

-

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

Katso 1- ja 9-kohdan vastaukset.

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

-

Perko Jari
Asiakkuusmarkkinointiliitto ry