

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?

Ei ole näyttöä siitä, että sisämarkkinat olisivat merkittävästi tehostuneet tietosuoja-asetuksen ansiosta. Huolimatta tavoitteena olleesta digitaalisten sisämarkkinoiden yhdenmukaistamisesta, kansallisessa sääntelyssä on edelleen runsaasti vaatimuksia, jotka poikkeavat eri jäsenmaiden kesken merkittävästi toisistaan.

Haasteena yleisen tietosuoja-asetuksen soveltamisessa on myös siinä annettujen monien yksityiskohtaisten velvollisuuksien käytännön toteuttaminen. Esimerkiksi sopimusvelvoitteissa vaatimukset ovat liian yksityiskohtaisia, mikä aiheuttaa joillekin jäsenillemme käytännön haasteita olemassa olevissa ja tietosuojan näkökulmasta jo tarkoituksenmukaisesti toimivissa palveluissa. Sisämarkkinoiden tehostaminen ei edellytä kaikissa tilanteissa yksityiskohtaista, erittäin räätälöityä sopimista tietosuojasta. Tämän osoittaa jo se, ettei kuluneessa ajassa ole saavutettu toimivaa markkinakäytäntöä tietosuojan yksityiskohtaisen sopimisen toteuttamisesta. Myös anonymisoinnin ja pseudonymisoinnin vaatimukset ovat kohtuuttomat ja epäselvät.

Henkilötietojen tietoturvaloukkauksista ilmoittamisen määräaika koetaan myös epätarkoituksenmukaisen tarkaksi velvoitteeksi. 72 tunnin määräaikavelvoite estää poikkeamatilanteessa tapahtuneen tarkoituksenmukaisen tutkinnan ja toiminnan sekä johtaa monesti vääriin tulkintoihin ja tarpeettomiin ilmoituksiin.

Kaikilla yrityksillä ei välttämättä ole kykyä vastata kaikkiin tietosuoja-asetuksen perusteella tai jopa täysin perusteetta tehtyihin yksittäisten ihmisten vaatimuksiin. Suurilla yrityksillä on sekä kompetenssi että resurssit keskustelujen hoitamiseksi, mutta varsinkin pienten yritysten kohdalla osa vaatimuksista lähentelee jopa haitan- tai kiusantekoa. Tietosuoja-sääntelyn velvoitteita tulisikin

eriyttää nykyistä riskiperusteisemmin, jolloin suuriin henkilötietointensiivisiin toimijoihin kohdistettaisiin enemmän velvoitteita kuin pieniin henkilötietokeyyisiin toimijoihin.

Erityisesti julkishallinnossa erilaisia ohjeita ja suosituksia tulkitaan kuin ne olisivat pakottavaa sääntelyä, eikä tietosuoja-asetuksen riskiperusteisuutta ymmärretä oikein. Harvoin hyödynnetään toisen ministeriön tai viraston työtä, vaan lähdetään aina nollasta, ja turvaudutaan ulkopuolisiin konsultteihin. Tähän saadaan toivottavasti apua valtiovarainministeriön ja DigiFinlandin Cirrus-hankkeesta.

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

-

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?

Suomen tietosuojalakiin ei ole kirjattu kaikkia aikaisempia ja tietosuojallisesti tarkoituksenmukaisia käsittelyperusteita. Lainsäädännössä on tältä osin kehitettävää. Koska julkisyhteisöille ei nykyisin voi määrätä seuraamusmaksuja, ne ovat osoittaneet piittaamattomuutta tietosuojan vaatimuksista. Hallitusohjelmaan on onneksi kirjattu tavoite säätää hallinnolliset sakot tietosuojaloukkauksista koskemaan yhtäläisesti julkista ja yksityistä sektoria.

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?

Kansallinen ePrivacy-direktiivin täytäntöönpano (laki sähköisen viestinnän palveluista) ja yleinen tietosuoja-asetus ovat paikoin ristiriidassa keskenään. Tämä ja eri viranomaisten toimivaltuuksien rajat sekä vaihtelevat tulkintakäytännöt aiheuttavat haasteita sähköisiä viestintäpalveluita tarjoaville toimijoille. Lisäksi jo vuosia jatkunut epäselvyys tulevan ePrivacy-asetuksen sisällöstä ja aikataulusta heikentää toimijoiden kykyä valmistautua etukäteen tuleviin vaatimuksiin.

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

Tietosuoja-asetuksen soveltamisessa on EU:ssa poikkeavia oikeuskäytäntöjä, ja sitä tulkitaan eri jäsenvaltioissa eri tavoin. Erilaiset asetuksen perusteella annetut tuomiot eri puolilla unionia ovat ristiriidassa keskenään. Erilaisen oikeuskäytännön takia eri maiden viranomaisten antaman ohjeistuksen ja kannanottojen sitovuudesta ja soveltamisesta esimerkiksi Suomessa vallitsee epävarmuus.

Lisäksi paikalliset viranomaiset voivat vaatia asetuksen vaatimuksia ylittäviä menettelytapoja, kuten tietosuojavaltuutetun toimiston erittäin yksityiskohtainen ja laaja henkilötietojen tietoturvaloukkauksen ilmoituslomakkeen tietosisältö. Suomessa vaaditaan loukkausilmoitusta huomattavan matalalla kynnyksellä, vaikka usein ilmoitukset eivät johda mihinkään, vaan niitä kerätään lähinnä mielenkiinnon vuoksi. Tämä on omalta osaltaan johtanut viraston jatkuvaan resurssipulaan ja käsittelyaikaisten venymiseen. Tarkoituksenmukaisempaa olisi keskittyä loukkausilmoitukseen, joilla voidaan edistää yleisen tietosuoja-asetuksen perimmäisiä tavoitteita: vahvistaa EU:ssa asuvien henkilöiden oikeuksia omiin henkilötietoihinsa sekä yksinkertaistaa sääntely-ympäristöä niin, että sekä EU:n sisäinen että kansainvälinen liiketoiminta helpottuisivat.

Suomessa on myös hyvin erilainen, muita maita tiukempi tulkinta esimerkiksi siitä, miten pseudonymisointia voidaan hyödyntää. Tietosuoja-asetuksen vaatimuksia huomattavasti tiukempi tulkinta tekee datataloudesta ja datan hyödyntämisestä esimerkiksi terveydenhuoltosektorilla sekä tutkimuksessa lähes mahdotonta. Yksityisyydensuoja ohittaa jo mahdollisuuden parempaan tietoturvaan tai potilaan oikeuden saada kehittyneempää hoitoa. Liian tiukka tulkinta estää esimerkiksi terveysteknologiayritysten mahdollisuudet myydä sovelluksiaan tai tehdä kansainvälistä yhteistyötä. Hallitusohjelmassa on onneksi tavoitteena kumota tiedon liikkuvuutta, pilvipalveluiden tarkoituksenmukaista käyttöä tai muuten julkisten palveluiden tarkoituksenmukaista järjestämistä haittaavat säädökset ja hyödyntää tarvittaessa nykyistä laajemmin GDPR:n kansallista liikkumavaraa.

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

-

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?

-

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?

-

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

-

Metsola Asko
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry