

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?

Energiateollisuus ry (ET) kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan seuraavaa:

Yleisellä tasolla tietosuoja-asetuksen hyödyt liittyvät henkilötietojen suojan yhdenmukaistumiseen EU:n alueella sekä viranomaisten yhteistyöhön.

Tietosuoja-asetuksen soveltamisessa merkittävimpiä haasteita on lukuisten epäselviksi koettujen säännösten tulkinta sekä yksityiskohtaisten velvollisuuksien käytännön toteuttaminen yritystasolla. Asetus on tekstiltään monissa kohdin niin avointa, että sen soveltaminen koetaan vaikeaksi ja toimintatapojen oikeellisuudesta varmistumiseen liittyy yhä merkittävää oikeudellista epävarmuutta.

Myöskään tietosuoja-asetukseen liittyvää viranomaisneuvontaa ei ole koettu riittäväksi. ET katsoo, että yritysten neuvontaan tulee panostaa, jotta asetusta noudatetaan myös tulevaisuudessa. Yritysten tulisi saada nykyistä konkreettisempia neuvoja tietosuoja-asetuksen soveltamisesta.

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

ET katsoo, että haasteelliseksi on koettu muun kansallisen lainsäädännön soveltaminen yhdessä tietosuojalain kanssa. Esimerkiksi suostumuksen käsitteen voi tulkita tarkoittavan tietosuojalaissa eri asiaa kuin jossakin muussa kansallisessa erityislainsäädännössä, mikä tuo haasteita henkilötietojen käsittelyn käytännön toimintaan. Esimerkkeinä mainittakoon työelämän tietosuojalain (759/2004, erityisesti 4 §:n ja 3 luvun) asettamat vaatimukset suostumukselle ja sähköisen viestinnän palveluista annetun lain (917/2014) vaatimukset suostumukselle paikkatiedon käyttöön liittyen.

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?

-

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?

-

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

Lähtökohtaisesti yleisen tietosuoja-asetuksen hyödyt liittyvät yhdenmukaiseen ja harmonisoituun sääntelyyn jäsenvaltioiden välillä. On kuitenkin havaittu, että asetuksen soveltamisessa ja sen tasossa eri jäsenvaltioissa on verrattain isoja eroja.

Lisäksi lainvalinnan osalta rajat ylittävissä tilanteissa on koettu paikoin epäselväksi, miten tietosuoja-asetusta sovelletaan päällekkäin eri maiden erityissääntelyn (esim. markkinointi- tai kuluttajansuojasääntelyn) kanssa.

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

Yleisesti ottaen ET pitää tietosuojaneuvoston antamia ohjeita hyödyllisinä antamaan suuntaa soveltamiseen, ja ne helpottavat asetuksen käytännön soveltamista jonkin verran. ET:n näkemys on, että monet olemassa olevat ohjeet on kuitenkin koettu liian monitulkintaiseksi ja yleisluontoisiksi eivätkä ne näin ollen auta yrityksiä riittävästi säännösten käytännön soveltamisessa ja ratkaisujen tekemisessä.

On lähtökohtaisesti hyvä, että tietosuojaneuvosto on sisällyttänyt ohjeisiin käytännön esimerkkejä, mutta nykyisistä esimerkeistä ei usein löydy yritysten konkreettisiin tosielämän tilanteisiin sopivaa esimerkkiä. Esimerkiksi jo olemassa olevasta ohjeistuksesta huolimatta henkilötietojen tietoturvaloukkauksien osalta pidetään paikoittain yhä epäselvänä, miten luonnollisten henkilöiden oikeuksille ja vapauksille aiheutuvaa riskiä on arvioitava - eli tuleeko tietoturvaloukkauksesta ilmoittaa vai ei.

Artiklan 30 'seloste käsittelytoimista' osalta on kaivattu selkeytystä ja seikkaperäisiä esimerkkejä erityisesti siihen, millä tasolla artiklassa mainitut tiedot tulee antaa.

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?

Epäselväksi on koettu mm. se, että millä tasolla rekisterinpitäjällä on vastuu koko alihankintaketjun tiedonsiirroista ja miten koko alihankintaketjun arviointi tulisi käytännössä todentaa esimerkiksi vaikutustenarvioinneissa. Rekisterinpitäjien on paikoitellen varsin hankala arvioida alihankkijoittensa ja ketjussa näiden alihankkijoiden välisiä sopimussuhteita sekä saada tietoa niihin liittyvistä riskeistä. Haasteellisiksi on koettu myös tilanteet, joissa henkilötietoja siirretään kansainvälisen liiketoiminnan pyrittämisen yhteydessä kolmansiin maihin.

Monet tietosuoja-asetuksen mukaiset mekanismit nähdään yrityksissä työläinä ja niihin sisältyy paljon epävarmuuksia. Näistä mekanismeista erityisesti henkilötietojen siirtojen vaikutusarviointien (TIA) tekeminen on koettu yrityksissä käytännössä hyvin haastavaksi ja kuormittavaksi. Esimerkiksi kohdemaan lainsäädännön analysointi vaatii resursseja, joita harvalla yrityksellä on käytössä.

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?

On noussut esiin, että rekisteröidyn näkökulmasta ei ole selvää, milloin kolmannen maan yritys joutuu soveltamaan asetusta ja milloin ei, koska yritykset, jotka eivät sovelle asetusta, eivät joudu sitä ilmoittamaan. Käytännön esimerkkinä normaalisti henkilötietojen käsittelijänä EU:n ulkopuolella toimiva alihankkija voi tulla sidotuksi tietosuoja-asetukseen sopimusten kautta. Sama EU:n ulkopuolella toimiva alihankkija saattaa tarjota palveluaan (esim. IT-tuki) vain yritykselle, mutta pyytää yrityksen työntekijöiltä palautetta yritykselle tarjoamastaan palvelusta ns. rekisterinpitäjän roolissa. Tällöin on asetuksen nojalla epäselvää, tuleeko tietosuoja-asetus artiklan 3(2b):n mukaan sovellettavaksi, sillä kyseessä ei ole suoraan työntekijöille tarjottu palvelu.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Useat tietosuoja-asetuksen 4 artiklan mukaiset määritelmät koetaan epäselviksi ja vaikeiksi tulkita käytännön soveltamistilanteissa. Esimerkiksi terveystiedon käsite on epäselvä ja eriävää viranomaisten tulkintakäytäntöä on siitä, onko esimerkiksi tieto henkilön sairaslomasta terveystietoa.

Asetuksen jaottelu artiklassa 4(7 ja 8) rekisterinpitäjän ja käsittelijän rooleihin on koettu mustavalkoiseksi ja määritelmiä pidetään liian abstrakteina ja yleisluontoisina suhteessa käytännön elämän soveltamiseen. Yritysten käytännön elämässä henkilötietojen käsittelijät toimivat lähes aina myös rekisterinpitäjinä. Tämä konkretisoituu esimerkiksi palautteen tai lokitietojen keräämisessä ja tuotekehityksessä. Ks. tältä osin myös lausunnon kommentti koskien lukua IV.

Artiklassa 4(23) 'Rajat ylittävä käsittely' puhutaan "rekisterinpitäjän" toimipaikoista ja toiminnasta, vaikka käytännössä konserneissa on usein eri toimintamaissa erilliset yritykset, jotka toimivat yhtäältä rekisterinpitäjinä, mutta toisaalta myös osallistuvat samaan käsittelyyn (esim. konsernin HR-järjestelmät). Rekisterinpitäjä on yleensä yksi oikeushenkilö, näissä tilanteissa käytännössä oikeushenkilöitä on monia. Tältä osin epäselväksi on koettu, koskeeko rajat ylittävä käsittely myös näitä tilanteita.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Artiklaan 5(2) sisältyvä osoitusvelvollisuus on kohtalaisen raskas ja asetuksen tekstin perusteella on haasteellista saada varmuutta siitä, milloin esim. osoitusvelvollisuus täytetty riittävällä tasolla. Osoitusvelvollisuuden osalta olisi tärkeää saada viranomaiselta ohjeistusta siitä, mikä on minimitaso.

Lisäksi artiklan 5(1f) mukainen oikeutettu etu käsittelyperusteena on koettu hankalasti ymmärrettäväksi. Käsittelyperusteiden osalta on myös pidetty epäselvänä, että voiko artiklan 6(1b) mukaista sopimusta käyttää henkilötietojen käsittelyn perusteena B2B-tilanteissa. Artiklan sanamuodon mukaisesti voi tulkita, että sopimusta saa käyttää käsittelyperusteena ainoastaan silloin, jos sopimusosapuolena on rekisteröity. Käytännössä henkilötietojen käsitteleminen voi olla tarpeen sopimuksen hoitamiseksi myös sellaisissa B2B-tilanteissa, joissa sopimus on tehty yrityksen kanssa.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Yrityksissä on koettu epäselväksi, miten ja missä käytännön tilanteissa artiklan 19 mukaista ilmoitusvelvollisuutta henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta tulisi soveltaa.

Artiklan 21 mukaisen vastustamisoikeuden osalta on kaivattu konkreettisia esimerkkejä, mitä tarkoitetaan 'henkilökohtaiseen erityiseen tilanteeseen liittyvällä perustelulla'. Kyseinen määritelmä on tulkinnanvarainen ja lisäksi on epäselvää, miten sellaisen tiedon kerääminen toimii minimointiperiaatteen kannalta. Käsityksemme mukaan muotoilun taustalla lienee hakukonekonteksti, mutta muissa käytännön tilanteissa, kuten henkilöstöhallinnossa, soveltaminen on koettu hankalaksi. ET toivoo tarkennusta tai viranomaisen ohjeistusta vastustamisoikeuden käyttöalaa erityisesti 'henkilökohtaisen erityiseen tilanteeseen liittyvän perustelun' osalta.

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

ET:n kokemuksen mukaan artiklan 26 mukainen yhteisrekisterinpitäjäyys ja sen tulkitseminen on aiheuttanut yrityksissä monenlaisia haasteita etenkin konserniyhtiöiden osalta. Energiayhtiöiden

joukossa on useita konserniyhtiöitä, joilla on yhteinen asiakastietojärjestelmä. Epäselväksi on esimerkiksi koettu se, milloin konserniyhtiöitä tulisi pitää itsenäisinä toisistaan irrallisina rinnakkaisina rekisterinpitäjinä vaiko yhteisrekisterinpitäjinä käsittelemiinsä henkilötietoihin nähden. Lisäksi on tulkinnanvaraista, voivatko kaksi rekisterinpitäjää käsitellä samoja henkilötietoja olematta yhteisrekisterinpitäjiä. Selkeytystä on kaivattu teemaan liittyen myös sen osalta, milloin kyseessä on yhteisrekisterinpitäjyyden sijaan vain siirto rekisterinpitäjältä toiselle.

Haastavaksi koetaan myös rekisterinpitäjän ylikorostunut vastuu suhteessa henkilötietojen käsittelijään erityisesti henkilötietojen käsittelijän ollessa markkinajohtaja tai tämän tarjotessa alustapalveluja. Haasteita tuo se, että henkilötietojen käsittelijöillä on käytännössä monissa tilanteissa merkittävä valta henkilötietojen käsittelyssä rekisterinpitäjään verrattuna, vaikka rekisterinpitäjällä on suurempi vastuu tietosuoja-asetuksen noudattamisessa. Henkilötietojen käsittelijät voivat näin ollen vaikuttaa huomattavasti palveluiden tietosuojan toteutukseen, sillä ne eivät usein räätälöi tietosuojaominaisuuksia jokaiselle asiakkaalleen erikseen. Joidenkin henkilötietojen käsittelijöiden tarjoamiin palveluihin usein kuuluu valmiiksi rakennettuna rekisterinpitäjälle kuuluvien velvollisuuksien toteuttamista, joka toisaalta auttaa rekisterinpitäjää, mutta toisaalta antaa suhteetonta päätösvaltaa käsittelijälle vastuun pysyessä rekisterinpitäjällä. Esimerkiksi käsittelysopimusten ehdot sekä käytännöt rekisteröidyn informoinnin toteuttamiseen, suostumusten pyytämiseen tai säilytysaikoihin voivat tulla pitkälti suoraan vahvassa markkina- asemassa olevien käsittelijöiden sanelemana heidän oman formaattinsa mukaisesti.

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

-

Pynnönen Petra
Energiateollisuus ry

