Lausunto

06.09.2023

Kela 59/010/2023

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?

Soveltamiseen liittyvät merkittävimmät hyödyt

Yleinen tietosuoja-asetus on luonut yhtenäisen tietosuojasääntelyn viitekehyksen sekä yksityisen että julkisen sektorin toimijoille EU-jäsenvaltioissa. Yhtenäinen sääntely on edistänyt ja tukenut yhteisten käytänteiden luomista ja käyttöönottoa sekä parantanut rekisteröidyn oikeuksien ja vapauksien huomioimista henkilötietojen käsittelyssä. Henkilötietojen käsittelyn toteuttaminen ja siitä informointi on asetuksen myötä tullut läpinäkyvämmäksi ja

rekisteröidyt tunnistavat omia oikeuksiaan paremmin.

Tietosuoja-asetuksen soveltamisen aikana tietoisuus ja osaaminen tietosuojasääntelyn asettamista velvoitteista ja oikeuksista on kasvanut ja kehittynyt. Tämä on omalta osaltaan edistänyt tietosuojan sisään rakentamista organisaation toimintatapoihin. Myös valvontaviranomaisen tuottama informaatio ja ratkaisukäytäntö on saavuttanut laajan joukon toimijoita ja kasvattanut tietoisuutta tietosuojavaatimuksista. Tietosuojasta on tullut luonteva ja tärkeä osa jokapäiväistä työtä ja toimintojen kehittämistä ja sen asema luottamuksenrakentajana ja palvelujen laadun varmistajana on hyvin tunnistettu.

Asetusta edeltävä henkilötietolaki ohjasi hyvin henkilötietojen käsittelyä Suomessa, mutta kyseisen lain voimassaoloaikana moni organisaatio ei välttämättä kyennyt riittävällä tasolla todentamaan toimintansa lainmukaisuutta. Tietosuoja-asetus toi mukanaan osoitusvelvollisuuden vaatimuksen. Osoitusvelvollisuutta toteutettaessa monen organisaation toimintaa on korjattu ja kehitetty asiakasystävällisemmäksi ja läpinäkyvämmäksi. Tietosuoja-asetuksen soveltaminen on tuonut asiakkaan tarpeet ja oikeudet vahvemmin esille ja se on edellyttänyt jokaisen organisaation sisäisen arviointikyvyn kehittämistä riskilähtöisen ajattelutavan toteutumiseksi. Tämä on korostanut riskilähtöisen ajattelutavan merkitystä riskienhallinnan kehittämisessä ja henkilötietojen käsittelytoimissa.

Tietojen hyödyntäminen tapahtuu asetusta sovellettaessa entistä määrämuotoisemmin. Organisaatioiden turvallisuustasot ovat nousseet ja niissä on entistä paremmin havahduttu tietojen suojaamiseen, jotta organisaatio kykenisi ennakoimaan, vähentämään ja jopa poistamaan tahattomien riskien muodostumista ja välttymään ylimääräisiltä kustannuksilta sekä mahdolliselta rekisteröidyn oikeuksien loukkaamiselta.

Soveltamiseen liittyvät merkittävimmät haasteet

Soveltamiseen liittyvät merkittävimmät haasteet ovat liittyneet tietosuoja-asetuksen moniselkoisuuteen ja osittain sen tulkinnanvaraisuuteen. Myös tietosuoja-asetuksen paikoitellen vaikeaselkoinen kieliasu on aiheuttanut ajoittain haasteita. Tulkintoja koskevan epävarmuuden on koettu hidastavan digitalisaatiota ja aiheuttavan hallinnollista lisätyötä eivätkä asetusta soveltavat organisaatiot välttämättä saa miltään taholta tukea tekemilleen tulkinnoille. Edellä todetun ohella kansallisen valvontaviranomaisen ennakoiva ohjaus on koettu vähäiseksi ja riittämättömäksi. Valvontaviranomaisen roolia ennakollisessa ohjauksessa ja tulkintakäytäntöjä tukevana tahona tulisi vahvistaa. Myös tietosuojavastaavan rooli on useissa organisaatioissa edelleen epäselvä.

Tietosuojan ja toimivan julkisen hallinnon välillä tulisi käytännön soveltamisen yhteydessä löytää balanssi. Selkeällä lainsäädännöllä ja sen tulkinnoilla varmistetaan kansalaisten kannalta toimiva hallinto ja estetään ylimääräisiä kustannuksia hallinnolle ja kansalaisille. Tiedon liikkuvuudella on tärkeä rooli asiakkaille tuotettavissa palveluissa.

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

Tietosuoja-asetuksen 6 artiklan c alakohdan mukaan käsittely on lainmukaista, jos käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Artiklan e alakohdan mukaan käsittely on lainmukaista, jos se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

Henkilötietojen käsittelyperusteiden erottaminen kahden edellä todetun käsittelyperusteen välillä ei ole aina viranomaistoiminnassa yksiselitteistä. Haasteita lakisääteisen velvoitteen tulkinnassa aiheuttaa se, onko itse velvoite riittävän selvästi kirjoitettu ja millaisia keinoja rekisterinpitäjä voi lakisääteistä velvoitetta toteuttaessaan käyttää sekä minkä tyyppisiä henkilötietojen käsittelytoimia laissa säädetyn velvoitteen alle voidaan ylipäätään sisällyttää.

Kokonaisuutena arvioiden tietosuojalaki täydentää tarkoituksenmukaisella tavalla tietosuo-ja-asetuksen soveltamista ja luo toimivan viitekehyksen mm. tutkimukselliselle ja tilastolliselle henkilötietojen käsittelylle ja niihin liittyville rekisteröidyn oikeuksien toteuttamiselle.

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?

Erityislainsäädäntö näyttäytyy tietyissä tilanteissa monimutkaiselta kokonaisuudelta suhteessa tietosuoja-asetukseen. Erityislainsäädännössä ja laissa viranomaisten toiminnan julkisuudesta (621/199, jälj. julkisuuslaki) käytetään samoja käsitteitä kuin tietosuoja-asetuksessa, kuten esimerkiksi suostumus. Suostumus käsitteenä voi edellä todetuissa lainsäädännöissä ja tietosuoja-asetuksessa tarkoittaa eri asioita henkilötietoja käsiteltäessä, mikä tuo haastetta käytännön toimintaan.

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?

Kela katsoo, että julkishallinnossa yleistä tietosuoja-asetusta on pantu täytäntöön tehokkaasti ja onnistuneesti. Toisaalta toimeenpano on saattanut johtaa myös tehottomiin ja asiakkaan kannalta epätarkoituksenmukaisiin ratkaisuihin. Tietosuojan näkökulmasta tehokas ratkaisu saattaa johtaa muiden yleislakien näkökulmasta epätyydyttäviin ratkaisuihin.

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

Julkisuuslaissa säädetyt erilaiset henkilötietojen tiedonluovutus- ja antamistavat suhteessa henkilötietojen suojaan vaativat välillä yhteensovittamista. Aina ei ole myöskään yksiselitteistä, onko asiakkaan rekisteripitäjälle esittämässä pyynnössä kyse yleisen tietosuoja-asetuksen mukaisesta tarkastusoikeuden käyttämisestä vai julkisuuslain mukaisesta asiakirjapyynnöstä. Epäselvissä tilanteissa asiaa joudutaan selvittämään asiakkaan kanssa, jotta esim. tietojen toimittamisen määräaikoja ei ylitetä.

Edellä todetun ohella tietosuoja-asetuksen yhteensovittaminen myös muun yleisääntelyn sekä erityislainsäädännön kanssa aiheuttaa välillä tulkinnallisia haasteita. Kansalliset tulkinnat ovat välillä EU-sääntelyä tiukempia. Tästä esimerkkinä mm. kansallisessa automaatio-sääntelyssä oleva täysin automaattisen päätöksen määritelmä, joka on nykyisen ymmärryksen mukaan laajempi kuin tietosuoja-asetuksessa.

Rekisteröidyn suostumuksen asema tiedon luovuttamisessa vaatisi selkeytystä. Esimerkiksi julkinen hallinto käyttää suostumusta useimmiten ainoastaan tiedon luovuttamiseen. Kyse ei siis tässä yhteydessä ole suostumuksesta käsittelyn oikeusperusteena, sillä itse henkilötietojen käsittely perustuu lakiin. Epäselvän sääntelytilanteen vuoksi tieto liikkuu tällöin viranomaisten välillä rekisteröidyn suostumuksella.

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

Kelalla ei ole tältä osin lausuttavaa.

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

Euroopan tietosuojaneuvoston ohjeet ovat auttaneet käytännön soveltamistilanteisiin liittyvien ratkaisujen tekemisessä. Erityisen hyödyllisiksi on koettu kansainvälistä tiedonsiirtoa koskevat ohjeet (2/2020 ja 5/2021) ja ohje tietoturvaloukkausten ilmoittamisesta (1/2021). Kansainvälistä tiedonsiirtoa koskeviin ohjeisiin kaivattaisiin vielä täydennystä siltä osin, kuinka toimia, jos kahdenvälinen tiedonvaihtoa edellyttävä sopimus kolmannen maan kanssa on ollut voimassa jo ennen yleisen tietosuoja-asetuksen voimaantuloa eli sopimuksen sisältämä tietosuojasäädös ei ole yleisen tietosuoja-asetuksen vaatimusten

mukainen.

Edellä todetun ohella kaivataan Euroopan tietosuojaneuvostolta ohjetta TIA:n (Transfer Impact Assessment, tiedonsiirtoja koskeva vaikutustenarviointi) tuottamisesta sen varmistamiseksi, että arvio tehdään kaikissa jäsenvaltioissa ja organisaatioissa samantasoisesti. Lisäksi kaivattaisiin esimerkkejä sisältävää ohjetta ”lakisääteisen velvoitteen noudattamisen” ja ”yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi”-käsittelyperusteiden välisestä rajanvedosta ja tulkintakäytännöistä.

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?

Kela ei ole ollut mukana laatimassa yleisen tietosuoja-asetuksen 40 artiklan mukaisia käytännesääntöjä.

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

Yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvä seuraamusjärjestelmä voitaneen katsoa Suomessa riittävän tehokkaaksi ja tarkoituksenmukaiseksi, kun otetaan huomioon julkiseen sektoriin ja julkista valtaa käyttäviin toimijoihin tietosuoja-asetuksen seuraamusjärjestelmän ohella kohdistuvat hallinnon toiminnan lainmukaisuutta ohjaavat säännökset, virkavastuu ja toimintaan kohdistuva laillisuusvalvonta.

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?

Kansainväliset tiedonsiirtomekanismit ovat sinällään toimivia, vaikkakin niiden soveltaminen vaatii organisaatiossa spesifiä osaamista ja tietosuojaresursseja. Erityisesti haasteita on tunnistettu tilanteissa, joissa jäsenvaltiolla on jo asetuksen voimaantulon yhteydessä ollut voimassa oleva kahdenvälinen sopimus kolmannen maan kanssa. Tällainen sopimus on itsessään tietosuoja-asetuksen 46 artiklan 2 (a) kohdan mukainen suojatoimi (viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline), mutta oletettavasti sitä ei kuitenkaan voitane käyttää tiedonsiirron perusteena, koska sopimuksen tietosuojasäädökset ovat ajalta ennen asetusta.

Kansainvälinen tiedonsiirto edellyttää lähtökohtaisesti TIA:n tekemistä. Tarkoituksenmukaista olisi, että tämä vaatimus edellytyksineen kodifioitaisiin myös tietosuoja-asetukseen, jotta kaikille asetusta soveltaville tahoille olisi selvää, mitä tällaiselta arviolta odotetaan. Näin voitaisiin varmistua siitä, että TIA:t tehtäisiin samantasoisesti kaikissa organisaatioissa. Mikäli TIA:a ei tuotaisi asetuksen tasolle, olisi tarkoituksenmukaista, että Euroopan tieto-suojaneuvosto laatisi ohjeen TIA:n tekemisestä ja TIA:lta vaadittavilta edellytyksiltä.

Mikäli ei voida varmistua siitä, että tietoja tullaan kolmannessa maassa käsittelemään EU:n tietosuojaa vastaavalla tasolla, ei henkilötietoja saa siirtää kolmanteen maahan. Tämä voisi pahimmillaan johtaa siihen, että viranomainen ei kykene hoitamaan lain tai kansainvälisten sopimusten mukaisia velvoitteitaan (esim. Kelan tapauksessa kahden välisiä sosiaaliturva-sopimuksia). Tiedonsiirrosta kolmansiin maihin on käyty keskustelua vuonna 2017 pide-tyssä EU:n 5. Forum on the International Dimension of Social Security Coordination -tilaisuudessa, jossa jäsenmaat ovat tuoneet esiin ennakoituja mm. kansainväliseen tiedonsiirtoon ja kahdenvälisiin sopimuksiin liittyviä ongelmia.

Kolmansien maiden toimijoiden henkilötietojen käsittelyn lainvaatimusten ja tietosuojatason varmistamiseen kuluu paljon työaikaa ja tämä vaatii eri asiantuntijoiden resursseja organisaatioissa. Edellä todetulla on vaikutusta kehitysprojektien ja hankintojen aikatauluun. Kansainvälisten tiedonsiirtojen suurimmaksi haasteeksi on tunnistettu niiden oikeudellinen epävarmuus, etenkin Yhdysvaltojen osalta. EU-tuomioistuimen ratkaisut ovat osoittaneet, ettei komission tekemien riittävyyspäätösten pysyvyyteen voi välttämättä pitkällä aikavälillä luottaa. Tästä syntyvä riski voi hankaloittaa merkittävästi erilaisten palveluiden käyttöönottoa.

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?

Kelalla ei ole tältä osin lausuttavaa.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Kelalla ei ole tältä osin lausuttavaa.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Yleisesti ottaen tietosuojaperiaatteet ovat auttaneet konkretisoimaan mm. niitä keskeisiä seikkoja, joita henkilötietojen käsittelyssä tulee huomioida, jotta käsittely vastaisi tietosuojasääntelyn vaatimuksia. Toisaalta periaatteissa käytetyt ilmaisut eivät kaikilta osin ole selkeitä ja voivat johtaa erilaisiin tulkintakäytäntöihin.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Yleinen tietosuoja-asetus on parantanut rekisteröidyn oikeuksia ja tehnyt rekisteröityjen henkilötietojen käsittelystä läpinäkyvämpää. Rekisteröityjen informointiin on selkeästi eri organisaatioissa panostettu, mutta edelleenkään sitä ei kaikilta osin anneta riittävän ymmärrettävässä muodossa. Selkeä ja tehokas informaatio vahvistaa rekisteröityjen luottamusta henkilötietojen käsittelyssä.

Tietosuoja-asetus ja tietosuojalaki mahdollistavat henkilötietojen käsittelyn viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi, kuten viranomaisen suunnittelu- ja selvittelytehtävät, jotka eivät kuulu varsinaisiin lakisääteisiin tehtäviin. Rekisteröidyllä on 21 artiklan mukainen oikeus vastustaa tietojen käsittelyä tässä yhteydessä, mutta oikeuden toteuttaminen tai siitä poikkeaminen voi osoittautua käytännössä haastavaksi ja hankalaksi.

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

Henkilötietojen tietoturvaloukkauksiin liittyvät vaatimukset asetuksessa ovat edellyttäneet määrämuotoisten prosessien, ohjeiden, toimintamallien ja kanavien luomista loukkausten ilmoittamiseksi ja niiden käsittelemiseksi. Määrämuotoinen prosessi ohjeineen on auttanut tunnistamaan poikkeamatilanteita ja kasvattanut organisaatioiden kyvykkyyttä poikkeamien ja niiden johdosta toteutettujen mahdollisten hallintatoimenpiteiden seurannassa ja hallinnassa.

Rekisterinpitäjyyttä koskevaan tulkintaan liittyvät haasteet ovat nousseet esille myös eräissä etuuksissa, joissa Kelan toiminta edellyttää laajaa palveluntuottaja verkoston käyttöä ja joissa varsinaisesta rekisterinpitäjyydestä ei ole säädöstä laissa.

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

Kela viittaa aiemmin kansainvälisten tiedonsiirtomekanismien ja tiedonsiirtojen kohdalla esittämäänsä.

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Valvontaviranomaisten riippumattomuus ja resurssit tulee turvata. Valvontaviranomaisen ennakolliselle ohjaukselle tulee antaa entistä enemmän painoarvoa.

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

Kelalla ei ole tältä osin lausuttavaa.

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

Rekisteröidyn oikeussuojakeinot ovat riittävän tehokkaita.

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

Tietojenkäsittelyyn liittyvät erityistilanteet on riittävällä tasolla huomioitu.

Hanhela-Lappeteläinen Leila
Kansaneläkelaitos