Elinkeinoelämän keskusliitto EK

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?

Elinkeinoelämän keskusliitto kiittää mahdollisuudesta lausua otsikossa mainitussa asiassa ja toteaa lausuntonaan seuraavaa.

Henkilötietojen käsittelyä sääntelevän EU:n yleisen tietosuoja-asetuksen 2016/679 (EU) (jäljempänä tietosuoja-asetus tai asetus) soveltaminen alkoi vuonna 2018. Asetuksen tarkoituksena on vahvistaa rekisteröityjen oikeuksia sekä tukea digitaalitalouden kehitystä sisämarkkinoilla yhdenmukaistamalla EU:n jäsenvaltioiden tietosuojasääntely.

Tietosuoja-asetus on kaikissa jäsenvaltioissa suoraan sovellettavaa oikeutta. Asetus jättää jäsenvaltioille kuitenkin joiltain osin myös kansallista liikkumavaraa. Suomessa asetuksen voimaantulon yhteydessä säädettiin kansallinen tietosuojalaki (1050/2018). Lisäksi sovellamme tieto-suoja-asetuksen rinnalla kansallista erityislainsäädäntöämme, kuten yksityisyyden suojasta työelämässä annettua lakia (759/2004).

Euroopan komissio toimittaa Euroopan parlamentille ja neuvostolle joka neljäs vuosi kertomukset yleisen tietosuoja-asetuksen arvioinnista. Tähän lausuntopyyntöön vastaamalla EK osallistuu osaltaan kyseiseen tietosuoja-asetuksen toimivuudenarviointiin.

Hyödyiksi voidaan laskea yhdenmukaisen sääntelyn EU:n jäsenvaltioiden välillä sekä eri viranomaisten välisen yhteistyön. Euroopan laajuinen tietosuojasääntelyn harmonisointi on helpottanut käytännön tietosuojatyötä. Johtavan tietosuojaviranomaisen määrittely ja nk. yhden luukun periaate ovat lisänneet oikeusvarmuutta ja poistaneet tietosuojadirektiivin aikaiset kansalliset käsittelytoimenpiteiden rekisteröintivaatimukset.

Tietosuoja ei ole asetuksen voimaantulon jälkeen ollut enää vain asiansa huolellisesti hoitavan yrityksen asia, sillä nyt kaikki henkilötietoja käsittelevät toimijat joutuvat ottamaan asetuksen velvoitteet huomioon toiminnassaan.

Asetus on pakottanut rekisterinpitäjät tekemään tietoinventaaria ja ymmärtämään, mitä henkilötietoja ne hallitsevat. Tämä näkyy muun muassa säilytysaikojen määrittelynä sellaisten tietojen osalta, joita aikaisemmin ei poistettu tietojärjestelmistä ainakaan säännöllisesti.

Tietosuoja-asetus on myös merkittävästi lisännyt kansalaisten yleistä tietoisuutta tietosuojasta. Tällä on ollut positiivinen vaikutus myös yritysten riskienhallintaan ja varautumiseen.

Toisaalta sisämarkkinoiden merkittävästä tehostumisesta tietosuoja-asetuksen ansiosta ei ole näyttöä. Huolimatta asetuksen tavoitteena olevasta digitaalisten sisämarkkinoiden yhdenmukaistamisesta jäsenvaltioiden kansallisissa sääntelyissä on edelleen runsaasti toisistaan poikkeavia vaatimuksia.

Asetuksen soveltamisessa haasteena on myös lukuisten ja yksityiskohtaisten velvollisuuksien käytännön toteuttaminen ja eriävät tulkintakäytännöt. Esimerkiksi sopimusvelvoitteita koskevat tietosuoja-asetuksen säännökset ovat liian yksityiskohtaisia. Myös asetuksen anonymisoinnin ja pseudonymisoinnin vaatimukset ovat kohtuuttomat ja epäselvät.

EU:ssa ollaan viimeistelemässä datasäädöstä, joka on teollista dataa koskeva perussäädös, jonka tavoitteena on vauhdittaa EU:n teollisuuden modernisointia. Valtaosa myös tästä teollisesta datasta tulee sisältämään henkilötietoja. Tästä syystä esimerkiksi anonymisoinnin ja pseudonymisoinnin käsitteiden selkeyttäminen tulee olemaan avain-asemassa myös eurooppalaisten yritysten kilpailukyvyn kannalta.

Yritysten on edelleen vaikea arvioida, mikä on asetuksen kannalta riittävä tietosuojan taso, ja löytää yhteistyökumppani, joka pystyy tämän vaatimustason toteuttamaan. Myös kansainvälisiin tiedonsiirtoihin liittyy edelleen oikeudellista epävarmuutta ja sellaisia vaatimuksia, joista aiheutuu yrityksille paljon työtä. Tämä työ ei ole aina oikeassa suhteessa todellisiin tietosuojariskeihin.

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

Tietosuojalaki on yleisesti ottaen toimiva, esimerkiksi siinä säännellyt dokumentointi- ja raportointivaatimukset ovat selkeitä. Haasteelliseksi koetaan EK:n näkemyksen mukaan enemmänkin muu kansallinen lain-säädäntö ja sen soveltaminen yhdessä EU:n tietosuoja-asetuksen ja tietosuojalain kanssa.

Haasteellista on, että hallinnollista seuraamusmaksua ei voida tietosuojalain mukaan määrätä valtion tai kunnan viranomaisille tai muille julkisoikeudellisille toimijoille. Sen sijaan tietosuojalain 24 §:n 5 momentin mukaan hallinnollinen seuraamusmaksu voidaan määrätä yritykselle vielä kymmenen vuotta tietosuojarikkomuksen tai laiminlyönnin tapahtumisesta.

Käytännössä seuraamusmaksu voidaan määrätä yksityisen sektorin toimijoille pidemmältä aikaväliltä, kuin asiaan mahdollisesti liittyvän tietosuojarikoksen syyteoikeuden vanhentumisaika on. Rikoslain mukainen syyteoikeus nimittäin vanhentuu kahdessa vuodessa, jos ankarin rangaistus on enintään vuosi vankeutta, sakkoa tai rikesakko.

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?

Yksityisyyden suojasta työelämässä annetussa laissa on tietosuoja-asetusta tiukempaa sääntelyä liittyen muun muassa työntekijöiden henkilötietojen käsittelyyn. Työelämää koskeva tietosuojalakimme on rajoittava jopa pohjoismaisessa kontekstissa, mikä aiheuttaa yrityksille haasteita kansainvälisten yhteistyökumppaneiden valinnassa.

Tulkintahaasteita aiheuttavat esimerkiksi kameravalvontaa koskeva lain 16 §, huumausainetestiä koskevat 7 ja 8 § sekä esimerkiksi se, että sanaa suostumus on käytetty työelämän tietosuojalaissa tavalla, joka ei näytä täyttävän yleisen tietosuoja-asetuksen ja siihen liittyvien eurooppalaisten viranomaisohjeiden ehtoja suostumukselle.

Suomessa on myös muita jäsenmaita tiukempi tulkinta siitä, miten pseudonymisointia voidaan hyödyntää. Tietosuoja-asetuksen vaatimuksia huomattavasti tiukempi tulkinta tekee datan hyödyntämisestä esimerkiksi terveydenhuoltosektorilla lähes mahdotonta. Liian tiukka tulkinta estää esimerkiksi terveysteknologiayrityksiä myymästä sovelluksiaan tai tekemästä kansainvälistä yhteistyötä. Yksityisyydensuoja ohittaa terveydenhuoltosektorilla ajoittain jopa potilaan oikeuden saada parempaa hoitoa.

Elinkeinoelämän keskusliiton näkemyksen mukaan asetuksen tarjoamaa kansallista liikkumavaraa ei edellä mainituista syistä ole Suomessa käytetty tarkoituksenmukaisella tavalla.

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?

Yritykset kokevat haastavana tietosuoja-asetuksen käsitteiden monitulkintaisuuden, kuten rekisterinpitäjän ja käsittelijän määritelmien abstraktiuden suhteessa käytännön elämään. Haastavaksi koetaan myös rekisterinpitäjän ylikorostunut vastuu suhteessa käsittelijään erityisesti käsittelijän ollessa markkinajohtaja tai tarjotessa alustapalveluja.

Sähköisten viestintäpalveluiden osalta ePrivacy-direktiivin täytäntöönpanon (laki sähköisen viestinnän palveluista (917/2014)) ja tietosuoja-asetuksen välinen epäselvyys sekä eri viranomaisten toimivaltuuksien rajat ja vaihtelevat tulkintakäytännöt aiheuttavat suuria haasteita alan toimijoille.

Tämä näkyy niin sähköisen suoramarkkinoinnin sääntöjen maakohtaisuutena kuin viestien luottamuksellisuutta koskevien tulkintojen erilaisuutena yhteisötilaajana toimivan työnantajan kannalta. Lisäksi vuosia jatkunut epäselvyys tulevan ePrivacy-asetuksen sisällöstä ja aikataulusta lisää epävarmuutta ja tekee alan toimijoille mahdottomaksi valmistautua etukäteen tuleviin vaatimuksiin.

Haasteita on ilmennyt esimerkiksi myös maksupalveludirektiivin ja tietosuoja-asetuksen yhteensovittamisessa. Ongelmat liittyvät etenkin viranomaisten ristiriitaisiin tulkintaohjeisiin. Myös rahanpesusääntelyn ja tietosuoja-asetuksen yhteensovittaminen on ollut käytännössä haastavaa.

Myös käsitys siitä, mikä on henkilötietoa, tuntuu olevan erittäin laaja, ja siihen liittyy edelleen epävarmuutta. Arvioinnissa tulisikin jatkossa korostaa enemmän riskiperusteisuutta. Jos esim. laitemittausdata on tulkittavissa henkilötiedoksi, mutta sitä käsittelee toimija, jolla ei ole kiinnostusta tiedon mahdolliseen henkilötietodimensioon, olisi tarkoituksenmukaisinta, että tilannetta ei tarkasteltaisi henkilötiedon käsittelynä.

Tietosuojasääntelyn velvoitteita tulisikin eriyttää riskiperustaisemmin. Ajatus korkeariskisten henkilötietojen suojaamisesta siten, että samalla vältetään vähäriskisten tietojen ylisuojaaminen, ei tällä hetkellä toteudu. Riskilähtöisyys ei toteudu käytännössä, koska esimerkiksi Suomessa viranomaiset ovat ottaneet tarpeettoman tiukkoja tulkintalinjauksia. Tämä on johtanut siihen, että yrityksissä käsitellään esim. s-postiosoitteita tietosuoja-asetuksen mukaisina suojattavina henkilötietoina niin, että se vaikeuttaa yritysten käytännön toimintaa.

Myös IP-osoitteen yksioikoinen tulkinta henkilötiedoksi aiheuttaa yrityksille haasteita. Voisikin olla tarpeen selkeyttää IP-osoitteiden eroa, esimerkiksi teollisuusympäristöjen IP-osoitteet tai muut laiteosoitteet, jotka eivät yleensä yhdisty luonnolliseen henkilöön. Kasvavien verkkoon kytkettävien laitteiden (IoT) määrän kasvaessa, IP-osoitteita ei tulisi EK:n näkemyksen mukaan tulkita jatkossa edes pääsääntöisesti henkilötiedoiksi.

Tietosuoja-asetuksen osalta perusoikeuspunninta olisi tarpeen: painotetaanko yksityisyyttä suojaavia oikeuksia jo kohtuuttomasti muihin perusoikeuksiin nähden, jopa siinä määrin, että ne heikentävät muiden oikeuksien toteutumista ja vaarantavat EU:n pyrkimykset kasvattaa data-taloutta ja edistää datan liikkuvuutta sisämarkkinoilla?

Henkilötietojen suojalla ei tule oikeusvaltiossa olla etusijaa esimerkiksi suhteessa sanavapauteen.

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

Tietosuoja-asetusta tulkitaan eri jäsenvaltioissa hyvin eri tavoin. Esimerkiksi tuomiot eri puolilla unionia ovat ristiriidassa keskenään, ja eri maiden viranomaisten antamien ohjeiden ja kannanottojen soveltamisesta Suomessa vallitsee yleinen epävarmuus.

Jäsenvaltioiden viranomaisohjeissa on eroavaisuuksia muun muassa siinä, mitkä käsittelytoimet vaativat niiden mukaan vaikutusten arviointia. Myös biometrisen informaation käytöstä käyttäjien tunnistamiseen on olemassa useita erilaisia tulkintoja ja ohjeita. Erot aiheuttavat yrityksille selvitystyötä ja lisäkustannuksia.

Esimerkiksi Suomessa vaaditaan loukkausilmoitusta huomattavan matalalla kynnyksellä, vaikka usein ilmoitukset eivät johda mihinkään, vaan niitä kerätään lähinnä mielenkiinnon vuoksi. Tämä on osaltaan johtanut tietosuojavaltuutetun viraston jatkuvaan resurssipulaan ja käsittelyaikojen venymiseen. Tarkoituksenmukaisinta olisikin keskittyä loukkausilmoituksiin, 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.

Myös evästeiden käyttöä ja evästeluvitusta on EK:n käsityksen mukaan tulkittu Suomessa tiukemmin kuin useissa muissa EU-maissa, mikä on omiaan asettamaan suomalaiset yritykset heikompaan asemaan liike-toimintaa tukevan asiakasdatan keräämisessä verkossa tapahtuvissa asiakastilanteissa.

Epäselvää on myös, minkä maan laki soveltuu tilanteissa, joissa rekisteröityjä on monissa maissa, tai kun tapaukseen sovelletaan tietosuoja-asetuksen rinnalla myös esimerkiksi kuluttajansuoja- ja markkinointi-sääntelyä; rekisteröidyn vai rekisterinpitäjän kotipaikan?

EK kiinnittää huomiota myös siihen, että EU:sta tulee enenevässä määrin lainsäädäntöä, joihin liittyvistä loukkauksista tulee tehdä ilmoituksia valvoville viranomaisille. Jatkossa sama loukkaustapaus voi laukaista velvollisuuden ilmoittaa asiasta tietosuoja-asetuksen, NIS2:n ja kyberresilienssisäädöksen mukaisesti. Ilmoitusten määrä ei enää palvele tarkoitustaan. Tulisikin

harkita ”yhden luukun” -toimintatapaa, jossa loukkausilmoituksen voisi tehdä esimerkiksi englannin kielellä, ja ruksia ne lait, jotka ilmoitukseen liittyvät, sekä maat, joihin katsoo ilmoituksen tarpeelliseksi reitittää.

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

Sekä EU:n että kansalliset tietosuojaviranomaiset eivät ole Elinkeinoelämän keskusliiton näkemyksen mukaan antaneet riittävän selkeitä ja käytännön tilanteita konkretisoivia ohjeita erilaisiin tulkintatilanteisiin.

Tietosuoja-asetuksen säännöksiä sekä tulkintoja tulisikin selkeyttää koko EU:n tasolla niin, että yritysten ei tarvitsisi arvailla ja käyttää paljon resursseja tulkintatilanteiden selvittämiseen. Pienillä yrityksillä ei tällaista mahdollisuutta edes ole.

Viranomaisten käytännönläheisellä ja aktiivisella neuvonnalla voitaisiin suuresti helpottaa yritysten työtä sekä poistaa oikeudellista epävarmuutta sääntelyn eri tulkintatilanteista. Tällä hetkellä yritysten saama tulkinta-apu jää erittäin vähäiseksi.

Esimerkiksi yhteisrekisterinpitäjyyden ja kansainvälisen tiedonsiirron edellytyksiä tulisi edelleen täsmentää epäselvyyksien välttämiseksi. Myös tietomurtojen ilmoitusvelvollisuuden raja on edelleen epäselvä, minkä lisäksi asetuksen 30 artiklan mukainen seloste käsittelytoimista kaipaisi selkeämpää ohjeistusta. Tarkempaa ohjeistusta tarvittaisiin myös tutkimukseen ja tilastointiin liittyvän käyttöperusteen tulkintaan liittyen (asetuksen resitaali 50).

Olemassa olevat ohjeet ovat EK:n näkemyksen mukaan liian monimutkaisia, eikä käytännön esimerkeistä useinkaan löydy tosielämän tilanteeseen sopivaa esimerkkiä. Ohjeita tuntuukin leimaavan varovaisuus, sillä esimerkeiksi on usein valittu varsin selkeitä tapauksia, joista ei ole juurikaan apua hankalien rajatapausten tulkinnassa. Toisaalta varovaisuus ilmenee siinäkin, että ohjeissa esitetyt tulkinnat näyttävät usein tarpeettoman tiukoilta käytännön toiminnan kannalta.

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?

Seuraamusmaksujärjestelmässä on haasteena se, että yrityksille voi syntyä raskaita seuraamuksia tahattomista tulkintavirheistä tai teknologisista häiriötilanteista, vaikka yritys olisi pyrkinyt toimimaan oikein. Siksi olisikin erityisen tärkeää, että viranomaiset antaisivat yrityksille tulkinta-apua

asetuksen soveltamiseen liittyvissä käytännön tilanteissa. Myös yritysten tekemä tietosuojatyö tulisi ottaa huomioon seuraamuksia arvioitaessa.

Pidämme ongelmallisena myös käsittelyaikojen pituutta ja viranomaisen reagoimattomuuden aiheuttamaa oikeudellista epävarmuutta, esim. tietoturvaloukkausilmoituksia koskien. Nopeammista päätöksistä olisi hyötyä myös muille toimijoille, jotka voisivat mukauttaa toimintaansa päätösten mukaisiksi.

Tarkastavan viranomaisen tulisikin EK:n näkemyksen mukaan ensin antaa ohjeita ja vasta niiden noudattamisen laiminlyönnistä tulisi sakottaa. Tämä olisi niin rekisteröityjen kuin rekisterinpitäjienkin etu.

Suomalaisen valvontaviranomaisen toiminta on toistaiseksi ollut reaktiivista ja pohjautunut kanteluihin, mikä ei välttämättä ole ohjannut viranomaisten huomiota asetuksen periaatteiden kannalta tärkeimmille alueille.

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?

Schrems II -ratkaisu EU:n tuomioistuimelta on aiheuttanut merkittävää epävarmuutta ja lisätyötä yrityksille. Maa-arviot ovat useimmille yrityksille erittäin vaativia. Olisikin luontevampaa, jos komissio voisi kantaa osavastuun maa-arvioista ainakin yleisimpien maiden osalta (USA, Intia, Kiina jne.). Esimerkiksi riittävää tietosuojan tasoa koskevat päätökset ovat olleet erittäin tervetulleita, ja niitä toivotaan lisää.

Lisäksi on epäselvää, millä tasolla rekisterinpitäjällä on vastuu koko alihankintaketjun tiedonsiirroista ja miten se tulisi käytännössä todistaa. Käytännön esimerkkinä ovat tiedonsiirtojen vaikutusarvioinnit, koska kohdemaan lainsäädännön analysointi vaatii resursseja, joita vain harvalla on käytössä. Haasteellisia ovat myös tilanteet, joissa henkilötietoja siirtyy kansainvälisen liiketoiminnan yhteydessä kolmansiin maihin, tietyissä tilanteissa niin, että niitä täytyy toimittaa suoraan viranomaisille lakisääteisistä syistä, vaikka se ei asetuksen ja tuomioistuintulkintojen mukaan olisi periaatteessa mahdollista.

Olisikin toivottavaa, että rekisterinpitäjän ja tietojenkäsittelijöiden kumppanien eli alikäsittelijöiden välistä suhdetta avattaisiin lainsäädännössä ja suosituksissa enemmän. Myös yritystä koskevien sitovien sääntöjen hyväksymismenettelyä tulisi sujuvoittaa. Mallisopimukset ovat sinänsä toimiva mekanismi, mutta niiden tulkinnassa tulisi paremmin sallia riskipohjaisuus.

Henkilötietojen kv-siirtojen puite on kokonaisuutena kohtuuttoman jäykkä, sillä se ei anna mahdollisuutta arvioida tietojensiirron todellista riskiä yksityisyyden suojalle, vaan kaikkia henkilötietoja tulee kohdella samalla tavalla. Tämä on erityisen haastavaa niille yrityksille, joilla on liiketoimintaa kolmansissa maissa. Onkin kestämätöntä, että varsinkin samanmielisten demokratioiden kesken tehtävät tiedonsiirrot ovat edelleen epävarmalla pohjalla. EU:n ja Yhdysvaltojen välinen Data Privacy Framework on erinomainen alku, mutta lisäksi tarvittaisiin EU:n ja Yhdysvaltojen välinen sähköisen todistusaineiston ja Cloud Act:n välinen yhteentoimivuus.

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?

Käsityksemme on, että esim. verkkokaupassa EU:n viranomaiset eivät ole riittävällä tavalla pystyneet varmistamaan sitä, että yritysten kilpailu tapahtuisi samoilla säännöillä EU:n ulkopuolelta toimiville ja EU:ssa toimiville yrityksille (Level playing field -haaste).

Palveluita käytettäessä suurtenkin suomalaisten yritysten on vaikeaa neuvotella jättiyritysten kanssa, jotka haluavat sanella, miten tietojenkäsittelysopimukset tehdään ja mitä käytäntöjä kv-tiedonsiirroissa ja käsittelyssä noudatetaan.

Näin ollen esim. amerikkalaiset yritykset määrittävät pilvipalveluissa käytetyn tietoturvan tason, mutta rekisterinpitäjänä tilaajat joutuvat kuitenkin vastaamaan mahdollisista sanktioista. Pidämmekin tärkeänä, että valvontaviranomaiset suuntaisivat valvontatoimenpiteitään myös isoihin käsittelijöihin, jotta käsittelijöille tulisi sitä kautta painetta nostaa tietoturvallisuuden tasoa ja jotta palveluntarjoajien määräävän markkina-aseman mukanaan tuomat haasteet ja riskit sopimusneuvotteluissa rekisterinpitäjän näkökulmasta eivät jäisi rekisterinpitäjän kannettaviksi.

Täytäntöönpanon ja vaatimusten yhdenmukaistaminen globaalisti selkeyttäisi tiedonsiirtoja ja niihin liittyviä vaatimuksia, minkä takia yhteistyön kehittäminen kolmansiin maihin olisi hyödyllistä.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Määritelmät ovat edelleen ongelmallisia, kuten ‘anonymisoitu/pseudonymisoitu tieto’. Edes tuomioistuimet eivät tunnu olevan yksimielisiä käsitteiden tulkinnasta, ja käännökset ovat huonoja. Suomenkielisessä versiossa on juututtu vanhan henkilötietolain käsitteistöön, vaikka asiat eivät aina vastaa toisiaan.

Anonymisoidun ja pseudonymisoidun tiedon määrittely ja ymmärryksen lisääminen esimerkiksi riittävästä pseudonymisoinnin tasosta ovat tärkeitä elementtejä teollisen datan hyödyntämisessä, ja uuden EU:n digi-datasääntelyn, kuten Data Actin, toimeenpanossa.

Myös ‘rekisterinpitäjän’ ja ‘henkilötietojen käsittelijän’ erottelu on hankalaa ja tarpeetonta. Velvoitteet voisivat koskea tasapuolisesti kaikkia henkilötietojen käsittelyyn osallistuvia toimijoita (esim. tietojen ETA-alueelta siirtäjä vastaa siirrosta, oli tämä sitten rekisterinpitäjä tai henkilötietojen käsittelijä).

Myös käsite ‘terveystiedot’ on hankala, koska käytännössä on hyvin vaikeata erotella, mikä tieto on terveystietoa. Onko esimerkiksi tieto siitä, että henkilö on sairaslomalla, terveystieto?

‘Rajat ylittävä käsittely’ artiklassa puhutaan ”rekisterinpitäjän” toimipaikoista ja toiminnasta, vaikka käytännössä konserneissa on usein eri toimintamaissa erilliset yritykset, jotka toimivat rekisterinpitäjinä mutta osallistuvat samaan käsittelyyn (esim. konsernin HR-järjestelmät). Epäselvää on, koskeeko rajat ylittävä käsittely myös näitä tilanteita.

Myös käsittelyperusteita tulisi olla mahdollista laajentaa alkuperäisestä esimerkiksi määräaikaista innovointia ja kokeilua varten. Tällä hetkellä kaikki paperityö täytyy tehdä ns. uusiksi, jos käsittelyperustetta halutaan muuttaa.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Periaatteiden tulkinta ja käytännön toteutus vaihtelevat, mistä aiheutuu yrityksille oikeudellista epävarmuutta. Vaikka rekisterinpitäjällä olisi tarkoitus noudattaa sääntelyä, se saattaa tulkita epämääräistä sääntelyä viranomaisen mielestä väärin ja päätyä hankaluuksiin.

‘Sopimusperuste’: Voiko sopimusperustetta käyttää B2B tilanteessa?

‘Rikostuomiotiedot’: Epäselvää, onko näiden tietojen käsittely sallittua sen jälkeen, kun ne ovat tulleet julkisiksi viranomaisen toimesta?

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Tulkintahaasteita voi tulla ainakin vastustamisoikeudesta. Jos rekisteröity ei tuo esille mitään omaan erityistilanteeseensa liittyvää perustetta, riittääkö rekisterinpitäjältä pelkkä tasapainotestiin viittaaminen ja sen saataville asettaminen? Entä miten henkilökohtaiseen erityiseen tilanteeseen liittyvän perustelun kerääminen onnistuu minimointiperiaatteen kannalta? Ilmeisesti muotoilun taustalla on internet / hakukonekonteksti, mutta sitä on erittäin hankala soveltaa muissa käytännön tilanteissa esim. HR kontekstissa.

Myös ‘henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus’ on epäselvä: Missä tilanteissa ja miten soveltuu käytännössä? Tosiasiassa rekisterinpitäjä voi olla monilla eri aloilla toimiva yritys, jonka tiedot ovat monissa eri järjestelmissä ja käytännössä eri

toimijoiden hallussa, vaikka rekisterinpitäjä nimellisesti on yksi kokonaisuus. Näin ollen rekisteröidyn oikeus kaikkiin omiin tietoihin yhdellä pyynnöllä voi olla haastava.

Kaikilla yrityksillä ei myöskään ole kykyä vastata kaikkiin tietosuoja-asetuksen perusteella tai jopa täysin perusteetta tehtyihin yksilöiden vaatimuksiin. Suurilla yrityksillä on sekä kompetenssi että resurssit keskustelujen hoitamiseksi, mutta varsinkin pienten yritysten kohdalla osa vaatimuksista lähentelee jopa haitantekoa. Tietosuojasääntelyn velvoitteita tulisikin eriyttää riskiperustaisemmin, jolloin suuriin henkilötietointensiivisiin toimijoihin kohdistettaisiin enemmän velvoitteita kuin pieniin henkilötietokevyisiin toimijoihin.

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

'Yhteisrekisterinpitäjät': Voivatko kaksi rekisterinpitäjää käsitellä samoja henkilötietoja olematta yhteisrekisterinpitäjiä? Milloin kyseessä on vain siirto rekisterinpitäjältä toiselle?

'Seloste käsittelytoimista': On epäselvää, millä tasolla tietojen tulee olla, siis pitääkö luettelossa mainitut asiat listata suhteessa toisiinsa (esim. riittääkö lista kaikista käsitellyistä henkilötiedon tyypeistä, vai pitääkö ne listata per käsittelyn tarkoitus, jne.)

'Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle': Jos loukkaus tapahtuu käsittelijällä, jolla on asiakkaina tuhansia rekisterinpitäjiä, olisi käytännöllisempää, jos käsittelijä tekisi ilmoituksen.

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

Asetuksen mekanismit ovat työläitä ja niihin sisältyy paljon epävarmuuksia. Liiketoiminta suorastaan haluaa välttää kv-tiedonsiirtoja, mikä voi vaikuttaa negatiivisesti yrityksen koko palveluvalikoimaan ja sitä kautta kustannuksiin.

Ylikansalliset palvelutarjoajat eivät myöskään usein toimi kuten EU-mekanismit edellyttäisivät. Palvelun käyttäjällä ei ole käytännössä juurikaan mahdollisuuksia ostaa vastaavaa palvelua muualta (kohtuulliseen hintaan), mutta se ei myöskään voi millään tavoin painostaa palveluntarjoajaa toimimaan asetuksen velvoitteiden mukaisesti (esim. alihankkijoista informointi ei yleensä toimi asetuksen esittämällä tavalla), vaikka siitä olisi kirjallisesti sovittu.

Rekisterinpitäjän vastuu alihankkijan toteuttamista siirroista jättää huomioimatta teknologia-alan isojen palveluntarjoajien markkinavoiman, sillä usein rekisterinpitäjällä on vaihtoehtoina joko hyväksyä palveluntarjoajan palveluun kuuluvat siirrot sellaisenaan tai jättää mahdollisesti liiketoiminnan kannalta hyvinkin kriittinen palvelu hankkimatta. Esimerkiksi tietosuoja-asetuksen 28 artiklassa taattu rekisterinpitäjän mahdollisuus vastustaa alihankkijan käyttöä ei auta asiaa, sillä

vastustusoikeus on useimmissa sopimuksissa toteutettu rekisterinpitäjän oikeutena lopettaa palvelun käyttö.

EU:n ulkopuolisten maiden lainsäädännön seuranta vaatii suomalaiselta rekisterinpitäjältä sekä juridisia että taloudellisia resursseja. Näitä ei pienillä yrityksillä edes ole. Komission tulisikin panostaa siihen, että se tekisi enemmän adequacy-tutkimuksia/päätöksiä. Nyt asia on sälytetty yksittäisten toimijoiden harteille.

Kolmannen maan viranomaisilta voi tulla kysymyksiä kansainvälisen yrityksen henkilöstöstä esim. verotukseen tai ammatillisiin sertifikaatteihin liittyen. Kyselyt voivat koskea komennuksilla kolmansissa maissa työskenteleviä työntekijöitä tai jäsenvaltioissa valmistukseen osallistuneita henkilöitä. Tähän liittyvää ohjeistusta tulisi myös olla lisää.

EK nostaa esiin myös sen, että EU:n tietoturvaviranomaisen (ENISA) luonnos pilvipalveluiden turvallisuuskriteeristöä (EUCS) sisältää suvereniteettivaatimuksia, jotka kytkeytyvät olennaisesti henkilötietojen siirtorajoituksiin, sillä esitetyt vaatimukset uhkaavat heikentää eurooppalaisten yritysten mahdollisuuksia toimia kansainvälisesti. Esitysluonnos vaikuttaisi toteutuessaan negatiivisesti myös kyberturvallisuuteen, kun EU-sertifioitujen datan siirtojen tarjoaminen kolmansiin maihin vaikeutuu. Tämä tulisi ottaa huomioon myös tietosuojasääntelyä koskevassa kokonaisarvioinnissa.

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Suomessa tietosuojaviranomainen (TSV) katsoo, ettei se voi neuvoa rekisterinpitäjiä, koska se on valvontaviranomainen. Muut viranomaiset Suomessa ja muiden maiden tietosuojaviranomaiset antavat enemmän ohjausta ja suoria neuvoja sekä kertovat hyvistä käytännöistä.

Olisikin toivottavaa, että myös TSV voisi ottaa kantaa esitettyihin toimintavaihtoehtoihin, jotta rekisterinpitäjä voi kerralla päätyä oikeaan ratkaisuun, eikä asia myöhemmin valituksen kautta tule arvioitavaksi, jolloin rekisterinpitäjä saa vain kehotuksen korjata toimintaansa asetuksen mukaiseksi, asiaa enempää täsmentämättä.

Kiinnitämmekin erityistä huomiota siihen, kun yritysten hallinnollista taakkaa kasvatetaan velvoitteilla, tulee samalla huolehtia viranomaistoiminnan tehokkuudesta niin, että lainsäädännön yhteiskunnallisiin tavoitteisiin myös päästään.

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

-

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

Olisi kohtuullista ohjata yrityksiä oikeaan toimintaan ennen sanktioita. Samalla valvontaviranomaisen tulisi täsmentää, mitä tämä pitää oikeana toimintana, eikä vain kehottaa rekisterinpitäjää toimimaan asetuksen mukaisesti. Tämä hyödyttäisi myös rekisteröityjä, sillä tietosuoja-asetuksen vastaiseksi tulkittava toiminta saataisiin korjattua aiemmin eikä vasta määräyksen ja sakkojen seurauksena.

Samalla ns. portinvartijatoimijoiden valvonta olisi keskitettävä komissiolle, koska tällä hetkellä kansallisilla tietosuojaviranomaisilla on kohtuuttoman iso vastuu, mutta vähäiset resurssit.

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

-

Huhtala Peppiina
Elinkeinoelämän keskusliitto EK