5.9.2023
Karvinen Tuulia

Finanssiala ry

VN/23585/2023
Lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

FA kannustaa selkeään sääntelyyn eurooppalaisella tasolla ja kansallisen tietosuojalain kokonaisuudistukseen

Henkilötietojen käsittelyä sääntelevä 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. Asetus on kaikissa jäsenvaltioissa suoraan sovellettavaa sääntelyä. Asetus jättää kuitenkin joiltakin osin jäsenvaltioiden lainsäätäjälle kansallista, asetuksen säännöksiä täsmentävää ja täydentävää sääntelyliikkumavaraa. Suomessa liikkumavaraa on käytetty 1.1.2019 voimaan tulleella tietosuojalailla (1050/2018) sekä sen rinnalla sovellettavalla erityislainsäädännöllä.

Euroopan komissio toimittaa Euroopan parlamentille ja neuvostolle joka neljäs vuosi kertomukset yleisen tietosuoja-asetuksen arvioinnista ja uudelleentarkastelusta. Tällä lausunnolla Finanssiala pyrkii tarjoamaan yleisiä ja nimenomaisesti finanssialaa koskevia näkemyksiä koskien tietosuoja-asetusta ja kansallista tietosuojalakia.

Finanssiala ry kiittää mahdollisuudesta lausua otsikossa mainitussa asiassa ja toteaa lausuntonaan seuraavaa.

1 Mitkä ovat olleet yleisen tietosuoja-asetuksen soveltamiseen liittyvät merkittävimmät hyödyt ja haasteet?

Finanssiala näkee tietosuoja-asetuksen merkittävimpinä hyötyinä, että tietosuojan ja yksityisyyden suojan arvo ovat nousseet Euroopassa laajempaan yhteiskunnalliseen keskusteluun ja edistänyt yksityisyyden suojaa Euroopassa merkittävästi. Ihmisten oikeutta yksityisyyteen kunnioitetaan uudella tavalla ja tekniikan rajoitukset eivät enää sanele kaikkea, vaan asioiden ratkaisemiseksi ponnistellaan aikaisempaa enemmän. Se on olennainen osa rekisterinpitäjien arkea ja toimintojen kehittämistä. Kuluttajat ja yritykset tunnistavat paremmin henkilötietojen käsittelyä koskevat vaatimukset, jotka ovat nykyään kaikille yhteneväiset eikä vain osaa toimijoista rasittava velvoite. Asetuksella nähdään olevan lisäksi positiivisia vaikutuksia riskienhallintaan ja varautumiseen.

Asetuksen olennaisimpina haasteina voidaan kuitenkin pitää sääntelyn vaikeatulkintaisuutta ja sitä, ettei tietosuoja-asetusta sovelleta jäsenvaltioiden välillä yhdenmukaisesti. Soveltamisen vaikeudesta kertovat Euroopan tietosuojaneuvoston (EDPB) yksityiskohtaiset ohjeet, joita on annettu yli 1000 sivua. Ohjeiden sisältämien lausumien oikeusperustaa ei voida myöskään kaikilta osin pitää täysin selvänä. Vaikka ohjeet eivät ole jäsenvaltioita velvoittavaa lain tai asetuksen tasoista sääntelyä, tietosuojaviranomaiset tukeutuvat ohjeisiin suuressa määrin antamissaan ratkaisuissa. Tämä tekee viranomaisvaatimusten sisällön seuraamisesta erittäin haastavaa.

Finanssiala toivoo, että viranomaisohjeistuksen sitovuutta ja oikeuslähdeopillista asemaa selvennettäisiin.

Tietosuoja-asetus rakentuu keskeisesti yleisille tietosuojaperiaatteille ja asetus lähtee riskiperusteisesta lähestymistavasta. Riskiperusteisen lähtökohdan mukaan tietosuoja-asetuksen velvoitteet ja vastaavasti suojatoimet on suhteuttava tietojenkäsittelystä aiheutuvaan riskiin. Tästä huolimatta tietosuojaneuvoston ohjeet ohittavat suurelta osin riskiperusteisuuden ja lähtevät puolestaan yksityiskohtaisesta, kasuistisesta ohjeistuksesta. Tietosuoja-asetuksen ollessa luonteeltaan yleisluonteinen ja soveltajalleen harkintavaltaa jättävä, aiheuttaa neuvoston ohjeiden yksityiskohtainen luonne oikeudellista epävarmuutta siitä, mikä on oikea menettelytapa. Todennäköisesti tämä tilanne tulee johtamaan entistä useammin pitkiin hallinnollisiin oikeusprosesseihin, kun selvyyttä joudutaan hakemaan tuomioistuimesta.

Tietosuoja-asetukseen sisältyy myös säännöksiä, joilla on osoittautunut olevan vähäinen merkitys käytännössä. Esimerkkinä voidaan mainita rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen (siirto-oikeus), oikeus rajoittaa tietojen käsittelyä sekä sertifiointia koskevat artiklat. Rekisterinpitäjiä koskevien velvoitteiden vaikutus asetuksella tavoiteltaviin seikkoihin vaihtelee esimerkiksi rekisterinpitäjän toimialasta ja toimintatavoista riippuen.

Tekemisten priorisointi ja mitoittaminen suhteessa asetuksen tavoitteisiin ja saataviin hyötyihin on ollut vaikeaa. Asetuksesta on seurannut paljon sellaistakin tekemistä, jonka todelliset hyödyt rekisteröidylle ovat vähäisiä ainakin finanssialalla. Sääntelystä seuraa hyvin paljon hallinnollista taakkaa, tarpeetonta byrokratiaa ja näin ollen lisäkuluja yhtiöille. Esimerkkinä tällaisesta tarpeettomasta hallinnollisesta taakasta nähdään muun muassa erilaisten arvioiden ja niiden dokumentoinnin toteuttaminen.

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

Finanssialan näkökulmasta haasteita tietosuojalain soveltamisessa liittyy sen 6 §:n erityisiä henkilötietoryhmiä koskevan käsittelyn 1-kohtaan, joka koskee vakuutuslaitoksen oikeutta käsitellä vakuutustoiminnassa saatuja tietoja vakuutetusta tai korvauksenhakijasta. Säännöksen sanamuoto tulisi selvyyden vuoksi muuttaa lain tarkoitusta vastaavaksi siten, että se kattaa yksiselitteisesti myös henkilön, jolle haetaan vakuutussuojaa.

Finanssiala katsoo, että erityisesti tilastointiin ja tutkimukseen liittyvä kansallinen sääntely on ollut vaikeaselkoista, eikä tietojen käsittely näissä tarkoituksissa selkeästi ratkea tietosuojalakia lukemalla. Haasteena nähdään myös kansallisen tietosuojalain tulkinnanvaraisuus ja suhde muuhun lainsäädäntöön sekä finanssialan vanhoihin alan ongelmattomiksi koettuihin toimintatapoihin nähden. Kansallisen sääntelyn toteuttaminen vaatii merkittävän määrän resursseja, jotka tuottavat hankaluuksia etenkin pienille ja keskisuurille toimijoille.

Kansallinen tietosuojalaki ei nykymuodossaan ole riittävän selkeä, mikä osittain johtuu suurella todennäköisyydellä siitä kiireestä, jonka puitteissa laki on säädetty tietosuoja-asetuksen voimaan tullessa. Lakiin on tuotu samoja pykäliä kuin mitä sisältyi aikanaan henkilötietolakiin ja täten hankaloittavat lain tulkintaa suhteessa muuhun

nykysääntelyyn. Tietosuojalain osalta tulisi toteuttaa huolellinen uudelleentarkastelu ja kokonaisuudistus oikeustilan selkeyttämiseksi.

Muilta osin tietosuojasääntelyn keskeisimmät haasteet löytyvät EU-tason säädöksestä eli tietosuoja-asetuksesta (ks. edellä kohta 1).

3 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?

Oikeusministeriön asettaman yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) työ jäi aiemmin kesken. Työryhmän tehtävänä oli esittää periaatteet kansallisen liikkumavaran tarkoituksenmukaisesta käytöstä ja koordinoida asiasta annetun erityislainsäädännön tarkistamiseksi tarpeellista lainvalmistelutyötä. Finanssiala kannattaa työryhmän työn loppuun saattamista ja kansallisen liikkumavaran käytön selvittämistä. Liikkumavaraa ei kuitenkaan tule käyttää siten, että Suomessa säädeltäisiin asiasta kansallisesti tiukemmin kuin muissa unionin jäsenvaltioissa. Tarpeettoman tiukka kansallinen sääntely luo epäsuhtatilanteita sisämarkkinoiden toiminnalle.

Työelämää koskeva tietosuojalakimme on rajoittava jopa pohjoismaisessa kontekstissa, mikä aiheuttaa yrityksille haasteita kansainvälisten yhteistyökumppaneiden valinnassa. Lakia yksityisyyden suojasta työelämässä ja sen 4 §:n muuttamista koskeva hallituksen esitys (35/2022) raukesi edellisellä hallituskaudella. Finanssiala kannattaa sääntelyn loppuun saattamista tältä osin työntekijän henkilötietojen keräämistä koskevaa sääntelyn selkeyttämiseksi. Tällä hetkellä kansallinen laki edellyttää työntekijän suostumusta tietojen käsittelyyn, kun tietoja kerätään muualta kuin häneltä itseltään pois lukien tilanteet, joissa asiasta säädetään suoraan laissa tai viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi. Työntekijän suostumus on käsittelyperusteena haasteellinen, koska tietosuoja-asetuksen mukaan suostumuksen ei pitäisi olla pätevä oikeudellinen peruste henkilötietojen käsittelylle sellaisessa erityistilanteessa, jossa rekisteröidyn ja rekisterinpitäjän välillä on selkeä epäsuhta.

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 koskien yksityisyydensuojaa ohittaa terveydenhuoltosektorilla ajoittain vakuutusyhtiöiden mahdollisuuden saada vakuutetun kohteen tietoja sellaisessakin tilanteessa, jossa vakuutettu on antanut suostumuksensa vakuutusyhtiöille tietojen käsittelyä varten.

4 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?

Finanssiala on panostanut tähän merkittävästi. Ala on raskaasti säännelty ja toimijat ovat pyrkineet edistämään myös tietosuoja-asetuksen velvoitteiden toimeenpanoa. Toisaalta, koska kaikki toimialat eivät ole pyrkineet samantasoiseen toimeenpanoon kuin Finanssiala, johtaa tämä epätasapainoon toimialojen välillä henkilötietojen käsittelyn toteutuksen osalta.

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

Haasteita on ilmennyt muun muassa maksupalveludirektiivin ja tietosuoja-asetuksen yhteensovittamisessa. Ongelmat edellä mainittujen sääntelyjen yhteensovittamisessa liittyvät vahvasti viranomaisten ristiriidassa oleviin ohjeistuksiin. EBA ja tietosuojaviranomainen ovat antaneet ohjeistuksia, joita ei ole mahdollista soveltaa yhtäaikaisesti. Myös EU-maiden pankkisalaisuussääntely ja tietosuoja-asetus eivät ole kaikilta osin yhteensopivia. Ongelmia ilmenee myös rahanpesusääntelyn ja tietosuoja-asetuksen yhteensovittamisessa, jotka vaikeuttavat väärinkäytösten ehkäisemistä nykysääntelyn valossa

Esimerkkinä voidaan mainita myös kestävän rahoituksen lainsäädäntökehikkoon kuuluva taksonomian ilmastosäädös ja vahinkovakuutuksen taksonomianmukaisuuskriteerinä tietojen yhteiskäyttöä koskeva kriteeri. Taksonomianmukaisuus tarkoittaa, että vakuutustuotteet täyttävät taksonomiassa luetellut kriteerit. Yksi kriteeri on, että vakuutusyhtiö jakaa vahinkotietoja yhden tai useamman viranomaisen saataville analyyttistä tutkimusta varten. Luovutuksen peruste on kuitenkin tietosuoja-asetuksen perusteella epäselvä, koska taksonomiasäädös ei sinänsä muodosta lakisääteistä velvoitetta tietojen luovuttamiseen.

Työeläketoimijan kannalta ongelmia tuottaa esimerkiksi heitä käytännössä velvoittavien viranomaisvaatimusten huomioon ottaminen silloin, kun asiaan liittyvien henkilötietojen käsittelytarpeiden taustalla ei ole suoraan lainsäädäntöön perustuvaa velvoitetta. Viranomaisen ohjeistusta ilman sääntelyn tukea ei voida pitää lakisääteisenä käsittelyvelvoitteena, jolloin arvioitavaksi tulee voidaanko tilanteessa soveltaa käsittelyn perusteena 6 artiklan oikeutettua etua. Haasteita seuraa ylipäätään siinä, että EU-sääntely ei juurikaan ohjaa tässä yhteensovittamistehtävässä viranomaisen ohjeistusten ja sääntelyn välillä. Sääntely on pyritty kirjoittamaan mahdollisimman selkeästi niin, etteivät eri säädökset ole ristiriidassa keskenään, mutta viranomaisen antamat ohjeistukset eivät toimialan kokemuksen mukaan ole olleet yhteensovittamisessa yhtä onnistuneita.

6 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. Nykytilan osalta on ilmeistä, että tietosuoja-asetusta sovelletaan eri jäsenvaltioissa eri tavoin. Lisäksi sakkoherkkyys ja suuruus vaihtelevat jäsenmaiden välillä huomattavasti. Muilta osin viittamme vastauksessa kohtaan 1.

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

Finanssiala näkee, että vaikka ohjeistuksen antaminen olisi yleisellä tasolla toivottavaa ovat neuvoston ohjeet auttaneet ainoastaan hyvin rajallisessa määrin soveltamisessa (ks. myös vastauksemme kohtaan 1). Finanssiala katsoo, että ongelmana on ohjeiden

tulkinnat, jotka menevät selkeästi tietosuoja-asetuksen asettamien velvoitteiden yli, eivätkä huomioi tietosuoja-asetuksen riskiperusteisuutta. Lisäksi osaa neuvoston tulkinnoista on myös todellisuudessa mahdotonta noudattaa (esimerkkinä rekisteröidyn oikeudet kattavat myös yritysten varmuuskopiointijärjestelmät).

Ohjeiden sitomattomuus ja epävarmuus käytännön soveltamisesta kansallisesti ja tuomioistuimissa tekee tulkinnasta ja soveltamisesta paikoin vaikeaa. Ei pitäisi jäädä rekisterinpitäjille tarvetta päättää noudatetaanko ohjeita vai ei. Tarkempaa ohjeistusta tarvittaisiin esimerkiksi tutkimukseen ja tilastointiin liittyvän käyttöperusteen tulkintaan liittyen (resitaali 50).

Finanssiala toivoo parempaa yhteistyötä eri viranomaisten välillä ja sidosryhmien kanssa edellä kuvatun viranomaiskohtaisen ohjeistusten ristiriitojen välttämiseksi (ks. myös vastauksemme kohdassa 5. tämän osalta). Lisäksi olisi toivottavaa, että viranomaisohjeistusta ja lainsäädäntöä valmisteltaessa viranomaiset kuuntelisivat sidosryhmiä. Usein lainsäädäntö tai viranomaisen ohjeistus ei ole pystynyt vastaamaan tosiasiallisiin käytännöntarpeisiin aiheuttaen tulkintaongelmien lisäksi haasteita soveltamisessa, kun käytäntö ja sääntely eivät kohtaa. Valmistelevat viranomaiset voisivat hyötyä toimialan antamasta käytännön kokemuksesta, jotta sääntelyyn ja ohjeistukseen saataisiin tosiasiallisesti toimivia ratkaisuja.

8 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?

Finanssiala ei ole ollut mukana laatimassa yleisen tietosuoja-asetuksen 40 artiklan mukaisia käytännesääntöjä, mutta olemme toimialan piirissä harkinneet tällaisten laatimista. Käytännössä merkittävimmäksi haasteeksi on muodostunut se, että Suomesta puuttuu tietosuoja-asetuksen 41 artiklan mukainen virallinen valvontaelin. On myös selvää, että tietosuoja-asetuksen mukaisten käytännesääntöjen tekeminen ja niiden soveltaminen vaatisi runsaasti taloudellisia panostuksia.

Finanssiala näkee myös epäsuhtaisena sen, että 41 artiklan mukaisen valvontaelimen perustaminen, valvonnan järjestely ja sanktioiden määrääminen mahdollisista rikkomuksista on käytännössä jätetty yksityisten toimijoiden vastuulle. Mikäli tietosuoja-asetuksen 40 artiklan mukaisia käytännesäätöjä toivotaan tosiasiallisesti käytettävän unionin laajuisesti, tulisi julkisen sektorin ja toimivaltaisen viranomaisen ottaa hoidettavakseen 41 artiklan mukaiset tehtävät.

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

Seuraamusjärjestelmän osalta Finanssialalla ei ole erityisiä toiveita, joskin tietosuojaviranomaiselta toivottaisiin avoimempaa ja ohjaavampaa otetta toiminnassaan.

Toimialalle on jossain määrin ollut pettymys, että tietosuojaviranomaisen ratkaisuissa ei anneta paljoa painoarvoa reaalimaailman haasteille ja palvelun sujuvuudelle sekä muille vastaaville seikoille. Ennen kaikkea toivottaisiin, että tietosuojaviranomaisen työssä heijastuisi enemmän ennakoivien ohjeiden tarjoaminen nykyisen sanktiopainotteisuuden sijaan. Varsinainen ennakkokuulemisprosessi on merkittävän

raskas ja hidas nykyisellään eikä täytä toimijoiden tarpeita ennakoivien ohjeiden saamiseksi. Lisäksi käsittelyajat ovat kohtuuttoman pitkiä nykyisellään, minkä nähdään heikentävän oikeusvarmuutta yritysten näkökulmasta. Viranomaisten resursseja tulisi tarkistaa käsittelyaikojen lyhentämiseksi.

Tietosuojalain 24 §:n 4 momentin mukaan: ”Seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.”

Julkisyhteisöt käsittelevät merkittävässä määrin kansalaisten arkaluontoisia tietoja koskien terveyttä, varallisuutta jne. ja ohjausvaikutuksen vuoksi nämä tahot tulisi säätää seuraamusmaksujen piiriin. Muissa EU:n jäsenvaltioissa näin on jo tehty ja julkisille toimijoille on myös määrätty merkittäviä seuraamusmaksuja niiden rikkomuksista. Julkisyhteisöjen jättäminen seuraamusjärjestelmän ulkopuolelle luo merkittävän epätasapainon julkisten ja yksityisten toimijoiden välille. Finanssiala tukee, että tietosuojaloukkauksista määrättävät hallinnolliset sakot laajennetaan koskemaan julkista sektoria yhtäläisesti yksityisen sektorin kanssa.

10 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?

Siirtojen edellyttämät mekanismit ovat raskaita ja byrokraattisia. Yksi EU:n tietosuoja-asetuksen alkuperäisistä tavoitteista oli EU-alueella toimivien yritysten kilpailukyvyn parantaminen. Tilanne kansainvälisten siirtojen osalta on ollut epäselvä koko asetuksen soveltamisen ajan ja tilanne on aiheuttanut rekisterinpitäjille jatkuvaa oikeusepävarmuutta sekä kustannuksia. Tässä suhteessa seuraukset yrityksille ovat olleet asetuksen alkuperäisten tavoitteiden vastaisia.

Tiedonsiirtomekanismit ja erityisesti mallilausekkeet lisäsuojatoimenpiteineen eivät ole toimivia. Haasteet liittyvät hallinnolliseen taakkaan ja työläisiin arviointeihin. Riittävyyspäätöksiä ja muita vastaavia tulisi olla enemmän. On käytännössä hyvin tehotonta, että jokainen yritys tekee itse lainsäädäntöselvityksiä kolmansista maista. Selvityksiin liittyy kustannuksia sekä oikeudellista epävarmuutta. Siirtymäajalle toimimiseen tarvitaan selkeämmät pelisäännöt. Merkitykseltään vähäisten henkilötietojen (esim. yhteystiedot) käsittelyn suojaaminen varsinkin kansainvälisten yritysten palveluja käyttöönotettaessa on kohtuuttoman työlästä. Vaatimukset asettavat jopa kohtuuttoman kynnyksen ottaa sinänsä tärkeitä palveluja käyttöön. Lisäksi epävarmuudet Yhdysvaltoihin menevien siirtojen osalta aiheuttavat suuria haasteita.

11 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?

Finanssialan käsityksen mukaan tämä on toimiva. Täytäntöönpanon ja vaatimusten yhdenmukaistaminen globaalisti selkeyttää siirtoja ja niihin liittyviä vaatimuksia, minkä takia yhteistyön kehittäminen kolmansiin maihin olisi hyödyllistä. EU:ssa

henkilötietojen suoja poikkeaa tasoltaan muista maanosista. Todennäköisesti tämä on joissain tapauksissa saattanut olla esteenä joillekin toimijoilla tulla EU:n markkinoille. Suuremmat yritykset ovat siirtäneet palvelimensa EU/ETA-alueelle, mutta tämäkään ei aina ratkaise kaikkia ongelmia. Myös EU:n oma datatalous ja -tuotanto saattaa kärsiä tiukasta sääntelystä. Finanssiala näkee, että tämä olisi selvittämisen arvoinen asia.

12 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.

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).

13 Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Finanssiala näkee, että henkilötieto-käsitteen uudelleentarkastelu olisi tarpeellista. Esimerkiksi pseudonyymin henkilötiedon käsittely henkilötietona täysimittaisesti/samojen velvoitteiden mukaisesti kuin suoraan tunnistettavissa olevien henkilötietojen käsittely, ei voida pitää kaikilta osin tarkoituksenmukaisena.

Edelleen se, että kaikki henkilöt, joita koskevia tietoja rekisterinpitäjällä voi jossain muodossa olla, ovat ”rekisteröidyn” asemassa, on käytännölle vieras. Jos esimerkiksi asianajotoimisto käsittelee perunkirjoitusta varten erinäisiä saldotodistuksia, aiempia perinnönjakokirjoja yms., niissä on yleensä runsaasti asiaan liittyvien henkilöiden tietoja. Nämä kaikki henkilöt eivät voi olla asetuksen tarkoittamassa rekisteröidyn asemassa siltä osin, että heihin voitaisiin soveltaa täysimääräisesti asetuksen sääntelyä (esim. informointivelvollisuus). Asetuksen soveltamisala on nykyisellään määritelty kattamaan lähtökohtaisesti kaiken sen kokonaan tai osittain automaattisen henkilötietojen käsittelyn, jota rekisterinpitäjä suorittaa. Tätä tulee rajata. Asetus kaipaisi kipeästi Suomessa aikaisemmin käytössä ollutta ns. liitännäishenkilöajattelua eli sen asian tunnistamista, että kaikki käsittelyyn sisältyvät henkilöt (esim. asiakirjoissa) eivät voi olla rekisteröidyn asemassa.

Myös erityisten henkilötietojen/arkaluonteisten tietojen käsittelyyn liittyy tiettyjä haasteita. Sopimus-oikeusperusteen pitäisi mahdollistaa arkaluonteisten tietojen käsittely silloin, kun palvelun ydinsisältö edellyttää kyseisten tietojen käsittelyä eikä erillistä suostumusta rekisteröidyiltä tällöin enää vaadittaisi. Palvelua ei yleensä voi tällöin käyttää ilman kyseisten tietojen käsittelyä.

Erityisesti 10 artiklan määrittelyjen tarkentaminen vaatisi huomioita. Esimerkkinä tästä voidaan antaa mitä tarkoitetaan ”Rikostuomio ja rikkomus”? Tulkinnat artiklan sisällöstä vaihtelevat huomattavasti EU:n alueella eivätkä ole yhteneväiset. On myös epäselvää, onko rikostuomiotietojen käsittely sallittua sen jälkeen, kun ne ovat tulleet julkisiksi viranomaisen toimesta.

Myös arkaluonteisten tietojen käyttö opetus/kehitystoiminnassa (esim. tekoäly) tulisi nimenomaisesti sallia, jotta asetuksen tavoitteet toteutuvat nykyaikana ja EU:n

digistrategian mukaisesti. Erityisten tietoryhmien käsittelyä koskeva 9 artikla on vaikeaselkoinen kokonaisuus (käsittelykielto ja siihen säädetyt poikkeukset) ja sitä koskeva resitaali ei selvennä asiaa juurikaan.

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

14 Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Rekisteröidyn oikeudet nähdään välillä haastavina soveltaa yksittäisissä tilanteissa, esim. tarkastusoikeuden osalta. Finanssiala näkee ne kuitenkin olevan osa asetuksen ydintä ja pääsääntöisesti ne toteuttavat asetuksen perimmäistä ajatusta. Osa oikeuksista (esim. siirto-oikeus) on jäänyt sivuraiteille ainakin vakuutusalalla, sen on pelätty aiheuttavan haasteita tulkinnallisesti.

Rekisteröidyn oikeuksia koskevaa sääntelyä ei voida pitää kaikilta osin onnistuneena. Oikeutta siirtää tiedot järjestelmästä toiseen ja oikeuttaa rajoittaa käsittelyä ei sovelleta käytännössä juuri lainkaan ja säännöksiä voidaan siten pitää tarpeettomina. Vuoden 2018 jälkeinen aika on osoittanut, ettei valtaosa rekisteröidyistä henkilöistä ole konkreettisesti tarvinnut näitä heille säädettyjä oikeuksia.

Oikeutettu etu ja siihen liittyvä vastustamisoikeus ovat epäselviä ja vaikeatulkintaisia sekä rekisterinpitäjälle että rekisteröidylle. Oikeutetun edun edellyttämää tasapainotesti/intressipunninta voidaan pitää haastavana tehtävänä, johon tarvitaan juridista asiantuntemusta. Rekisteröidyn voi myös olla hyvin haastavaa ymmärtää, mitä oikeutetulla edulla tarkoitetaan. Henkilötietodirektiivi ja henkilötietolaki sisälsivät aiemmin kielto-oikeuden koskien mm. sukututkimusta, mielipide- ja markkinatutkimuksia. Vastaavien selkeiden määritelmien palauttamista asetustekstiin voidaan pitää kannatettava niiden konkreettisuuden vuoksi.

Automaattista päätöksentekoa ja profilointia koskeva tietosuoja-asetuksen 22 artikla on muotoilultaan vaikeaselkoinen. Samoin automaattisen päätöksenteon ja profiloinnin käsitteet ovat epäselvät. Tietosuoja-asetus lähtee siitä, että automattinen päätöksenteko ja profilointi, jotka ovat tavanomaista tietojenkäsittelyä, muodostavat korkean riskin henkilötietojen käsittelylle ja ovat lähtökohtaisesti kiellettyjä. Tätä lähestymistapaa ei voida pitää perusteltuna enää tulevina vuosina - lisäksi se on ristiriidassa sen ajatusmallin kanssa, jota esim. EU:n datastrategia ilmentää (esim. tekoälyn laadukas hyödyntäminen). Automatisoinnin hyödyt tietojen käsittelylle, kuten inhimillisten virheiden väheneminen, tulisi huomioida.

Oikeus tietojen poistoon / oikeus tulla unohdetuksi tulisi määritellä asetuksessa siten, että siitä ilmenee mitä tietojen poistaminen käytännössä tarkoittaa ottaen huomioon poistettavien tietojen laajuus ja tietojen poistaminen esimerkiksi varmuuskopioilta. Nykyinen muotoilu antaa rekisteröidylle perusteettoman kuvan siitä, mitä kyseinen oikeus tarkoittaa. Esimerkiksi finanssialan toimijoiden on usein säilytettävä henkilötietoja joko lakiin perustuen tai yhtiön riskienhallintaan liittyvistä syistä eikä näitä voida poistaa, vaikka rekisteröity asiaa pyytäisi.

Ottaen huomioon jatkuvasti lisääntyvä tiedon määrä sekä digitalisoituva yhteiskunta ja toimintaympäristö, tulisi rekisteröidyn oikeuksia tarkastella myös kriittisesti.

Rekisteröidylle annettavien tietojen ymmärrettävyyttä ja tietojen käsittelyn läpinäkyvyyttä tulee kannattaa ja tähän panostaa. Kuitenkaan sitä, että esimerkiksi oikeus saada pääsy kaikkiin tietoihin toimittamalla rekisteröidylle kaikki häntä koskevat data-attribuutit eri tietojärjestelmistä ei voida pitää tarkoituksenmukaisena.

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.

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

Finanssiala katsoo, että tietoturvaloukkausten 72 tunnin aikarajaa voidaan pitää kohtuuttomana ottaen huomioon mm. ilmoitusten käsittelyaika viranomaisella sekä viranomaisen yleinen valmius antaa ohjausta varsinkaan teknisluonteisemmissa asioissa. Tietoturvaloukkausten ilmoitustarvetta kokonaisuudessaan ja niihin viranomaiselta saatavien vastausten hyödyllisyyttä olisi hyvä tarkastella kokonaisuudessaan uudelleen.

Vaikka roolit rekisterinpitäjä, käsittelijä, yhteisrekisterinpitäjä pitäisi olla selkeitä, niin tämän on katsottu aiheuttavan käytännön elämässä toimijoiden välillä jatkuvia haasteita. Valitettavan usein käytännöntilanteissa on havaittu eri kumppaneiden palveluita kilpailutettaessa, että samantyyppisessä toiminnassa isotkin toimijat ovat määritelleet nämä roolit täysin erilaisiksi. Asiasta löytyy hyvinkin laaja EDPB:n ohje, mutta kyseinen ohje ei tosiasiallisesti ole onnistunut ratkaisemaan näitä ongelmia.

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

Finanssiala näkee V luvun työläänä toteuttaa etenkin sen vuoksi, että luvussa suurena ongelmana nähdään riskiperusteisuuden puuttuminen, vaikka se on koko tietosuoja-asetuksen peruslähtökohta. Tämä aiheuttaa merkittävän määrän tarpeetonta työtä etenkin Yhdysvaltojen suuntaan sekä epävarmuutta ainakin näennäisesti sattumanvaraisesti osuvasta sanktioista.

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.

17 Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Suomessa tietosuojaviranomainen 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. Ennakollinen ohjeistus mahdollistaisi sen, että varsinaisilta rikkeiltä ja tietosuoja-asetuksen loukkauksilta voitaisiin välttyä ylipäänsä. Olisi suotavaa, että tietosuojaviranomainen valtuuksiin kuuluisi myös mahdollisuus ottaa kantaa ennakollisesti.

Ks. myös vastauksemme kohtaan 9.

18 Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

-

19 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.

Ks. myös vastauksemme kohtaan 9. ja 17.

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

Asetuksen sisältöä yleisesti koskevana kommenttina Finanssiala toteaa vielä, että asetuksen vaatimusten voisi toivoa kehittyvän periaatteellisempaan suuntaan. Tässä tarkoituksessa I ja II lukujen kehityksellä on olennainen tehtävä. Luvuista tulisi saada käytännönläheisiä, oikeusvarmoja ja niitä koskeviin resitaaleihin tulisi panostaa (tulkintaa ohjaava vaikutus). Lisäksi oikeusperustevalikoima on hyvin vaikea kokonaisuus, jota toivotaan selkeytettävän. Datan jatkohyödyntämistä erityisesti tilastollisissa ja tieteellisissä tarkoituksissa tulisi lisätä ja selkeyttää.

FINANSSIALA RY

Hannu Ijäs