FINANSSIALA

OM - oikeusministeriö

07.08.2019VN/5281/2019

Lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Väliotsikointi vastaa lausuntopalvelussa esitettyjä kysymyksiä.

Mitkä ovat olleet yleisen tietosuoja-asetuksen merkittävimpiä hyötyjä?

Merkittävimpänä hyötynä on pidettävä sitä, että asetus on parantanut rekisterinpitäjien henkilötietojen käsittelyprosesseja, järjestelmiä ja tiedon käsittelyn läpinäkyvyyttä. Tämä on kuitenkin lisännyt huomattavasti toimijoiden kustannuksia lyhyellä aikavälillä. Tehdyistä suurista investoinneista on kuitenkin mahdollista saada kustannussäästöjä ja liiketoimintahyötyjä pidemmällä aikavälillä.

Tietosuoja-asetuksen myötä tietosuojaa koskeva yleinen tietoisuus oikeuksista, velvollisuuksista ja vastuista on kasvanut. Tietosuoja-asetus ja siihen liittynyt mediahuomio on tuonut tietosuojakysymykset ja rekisteröidyn oikeudet paremmin kansalaisten tietoisuuteen ja toisaalta herättänyt rekisterinpitäjät korjaamaan ja parantamaan käytänteitään. Tietosuojasta informointi on merkittävästi parantunut tietosuojaselosteiden ja muun helposti saatavan informaation avulla. Rekisteröidyt käyttävät lisäksi aiempaa enemmän oikeuksiaan. Myös yleinen julkinen keskustelu henkilötietojen merkityksestä ja niiden väärinkäytöksiin liittyvien riskien hallinnan tärkeydestä on lisääntynyt.

Tietosuoja-asetuksen vaatimat panostukset ovat osaltaan lisänneet luottamusta finanssitoimialaan. Tietosuoja-asioihin panostaminen tukee myös pankki- ja vakuutussalaisuuden totuttamista sekä hyvää asiakaskokemusta. Finanssitoimialan yritykset näkevät, että tietosuoja-asetuksen mukaiset henkilötietojen käsittelyprosessit ovat pikemminkin kilpailuetu, eikä vain osa voimassa olevan lainsäädännön noudattamista.

Tietosuojan asema on noussut merkittävästi yrityksissä. Yritykset ovat nimittäneet tietosuojavastaavia, joilla on aiempaa selkeämpi asema, koska niiden rooli ja tehtävät on määritelty asetuksessa. Selkeä muutos on tapahtunut myös yrityksen johdon suhtautumisessa, sillä johto on ottanut tietosuojaa koskevat vaatimukset ja seuraamukset tietosuoja-asetuksen vaatimusten laiminlyönnistä vakavasti. Asetuksen vaatimien muutosten aikaansaaminen organisaatiossa on aiempaa helpompaa. Myös henkilöstön suhtautuminen tietosuojaan on parantunut ja osaamistaso lisääntynyt. Tietosuojan osaaminen yrityksissä onkin jakautunut aiempaa laajemmalle joukolle.

Tietosuojan priorisointi on näkyvillä myös kehittämisessä ja yhtiöiden riskien hallinnassa. Tiedonhallinta on yleisellä tasolla parantunut. Tietosuoja otetaan entistä paremmin huomioon tietojärjestelmien ja palveluiden kehittämisessä ja ylläpidossa ja tietosuojavaateet ovat osana hankkeen määrittelyä. Tietosuojan vaatimukset huomioidaan myös uusia tietojärjestelmiä sekä sovelluksia hankittaessa sekä erilaisissa toimintaprosesseissa. Tietosuoja-asetuksen mukainen toiminta luo

riskeistä tietoa, joka auttaa kohdentamaan ennalta ehkäiseviä toimenpiteitä. Lisäksi tietoturvaloukkauksista ilmoittamisen koetaan parantavan tietoturvan tasoa.

Mitkä ovat olleet yleisen tietosuoja-asetuksen soveltamisessa ja toimivuudessa suurimpia haasteita?

Sääntelyn tulkinnanvaraisuus

Finanssialan yritykset pitävät asetusta monilta osin niin tulkinnanvaraisena, että käytännön ratkaisuja on välillä vaikea rakentaa säännösten varaan. Tämä on johtanut markkinoilla osittain epäyhdenmukaisiin ja organisaatiokohtaisiin tulkintoihin, mikä luo oikeusepävarmuutta sekä rekisterinpitäjässä että asiakkaissa. Pahimmillaan asetuksen soveltaminen näyttää rekisteröidyn kannalta monitulkintaisina selosteina ja vaikeina oikeuksien toteuttamisen prosesseina.

Asetuksen abstraktiutta ja tulkinnanvaraisuutta on toisaalta yritetty kompensoida sillä, että asetuksesta on annettu runsaasti yksityiskohtaista viranomaisohjeistuista erityisesti Euroopan tietosuojaviranomaisten taholta. Suurimpana ongelmana näissä ohjeistuksissa on se, että niissä esitetään varsinaista asetustekstiä tiukempia tulkintoja. Lisäksi tulkinnoilla laajennetaan käsitteiden soveltamisalaa tarpeettomasti. Soveltamiskäytännön kehittymisen seuranta viranomaisten tulkintojen muodossa koetaan myös työläämmäksi kuin tarkkarajaisen sääntelyn seuraaminen, koska niitä ei aina julkaista systemaattisesti yhdessä paikassa.

Ongelmaksi on finanssialalla koettu myös se, että Euroopan tietosuojaviranomaisten tulkintaohjeistus ei ota kantaa toimialakohtaisiin eroihin. Toimialakohtaiset käytännöt ja erityispiirteet tulisi entistä enemmän huomioida viranomaisten ohjeistuksissa. Vaikka toimialojen laatimat mahdolliset omat käytännesäännöt auttavat soveltamisen haasteissa, eivät ne kuitenkaan poista viranomaisten tulkintojen aiheuttamaa epävarmuutta lain soveltamisesta.

EU-säädösten epäyhdenmukaisuus ja siitä aiheutuvat soveltamishaasteet näkyvät konkreettisesti esimerkiksi PSD2- ja GDPR-sääntelyiden välisessä epäselvässä suhteessa. Lisäksi terminologiat eriävät suhteessa toisiinsa, esim. suostumukselle kummassakin sääntelyssä on oma määritelmänsä, joka ei kuitenkaan ole yhdenmukainen.

Viranomaisohjeistusta on parannettava

Suurena ongelmana finanssialan toimijat pitävät sitä, että viranomaistahoilta on saatavilla soveltamiskysymyksissä käytännössä vain vähän tukea. Todennäköisesti resurssipulan vuoksi vastauksia ei saada riittävän nopeasti, sillä tietosuojavaltuutetun toimiston resurssit näyttävät rajallisilta työmäärään nähden. Jotta viranomaiset voivat parhaalla mahdollisella tavalla opastaa toimialaa, tulee niillä olla myös tarvittavaa toimialaosaamista.

Käytännössä on nähtävissä myös viranomaisohjeistuksen ja -linjausten ylätasoisuus tai niiden kokonaan puuttuminen. Asetuksen tulkinnanvaraisuus on johtanut poikkeaviin tulkintoihin eri maiden välillä myös viranomaispuolella. Kansallisten viranomaisten kesken on myös paljon eroa siinä, millaista ohjeistusta rekisterinpitäjille annetaan.

Sääntely on vaatinut toimijoilta suuren panostuksen

Tietosuoja-asetuksen soveltaminen on vaatinut kaikilta toimijoilta merkittävää panostusta sekä IT-järjestelmien että uusien prosessien ja toimintatapojen suunnittelun ja toteutuksen näkökulmista. Projektien lukumäärä ja niiden toteutukseen vaadittu henkilötyömäärä ovat olleet kokoluokaltaan erittäin merkittäviä. Lisäksi on panostettu asiakkaiden informoimiseen useissa eri kanavissa. Tietosuoja-asetuksen vaatimukset on huomioitu päivityksinä myös mm. asiakassopimusehdoissa ja tietosuojaselosteessa sekä toimittajien välisissä sopimuksissa.

Toimijat ovat myös panostaneet merkittävästi henkilökunnan sisäisiin koulutuksiin ja ohjeistamiseen. Myös yrityksen organisaatiorakenteeseen on saatettu joutua tekemään muutoksia, jotta tietosuoja-asetuksen vaatimukset voidaan huomioida parhaalla mahdollisella tavalla.

Kansallisen erityislainsäädännön myöhästyminen

Vakuutusyhtiöille on aiheutunut lisähaasteista kansallinen erityislainsäädännön myöhästymisestä, joka on rajoittanut väärinkäytösten rekisteröimistä ja johtanut sitä koskevan rekisterin väliaikaiseen poistamiseen toimijoiden käytöstä.

Tietoturvaloukkauksista ilmoittaminen

Sääntelyn tulkinnanvaraisuudesta hyvänä esimerkkinä on menettely tietoturvaloukkauksissa. Arviot viranomaisilmoituskynnyksen täyttymisestä vaihtelevat ja osa toimijoista ilmoittaa varmuuden vuoksi kaikista loukkauksista, osa arvioi ja määrittää ilmoitusvelvollisuuden riskiperusteisesti organisaation sisäisen näkemyksen mukaisesti, osa taas ei ilmoita loukkauksista lainkaan. Vastaavasti rekisteröidylle ilmoittamisen osalta viranomainen on käytännössä edellyttänyt suhteellisen matalaa ilmoituskynnystä huolimatta siitä, että asetus määrittää ilmoitusvelvollisuuden perusteeksi korkean riskin.

Finanssialan toimijoiden kokemuksen mukaan tietoturvaloukkausten dokumentointi ja niistä raportointi tietosuojavaltuutetulle on ollut työläämpää kuin mitä ennen asetuksen voimaantuloa osattiin ajatella. Suurin osa tietoturvaloukkauksista on käytännön kokemuksen mukaan yksittäisen työntekijän inhimillisiä virheitä, joissa yksittäisen asiakkaan tietoja päätyy väärälle henkilölle väärien yhteystietojen johdosta. Näiden ilmoittamista joudutaan harkitsemaan aina tapauskohtaisesti. Lisäksi joissakin tapauksissa useampi taho joutuu ilmoittamaan samasta loukkauksesta, kuten tilanteessa, jossa kyse on esim. virheestä e-laskujen toimitusprosessissa ja mukana on monta rekisterinpitäjää ja käsittelijää.

Finanssiala yritykset kannattavat sitä, että ilmoittamisen kynnys olisi viranomaiskäytännössä korkeammalla kuin nykyisin ja ilmoitusaika olisi määritelty työpäivissä. Jokaisesta yksittäisestä tapauksesta ilmoittaminen 72 h määräajassa ei ole tarkoituksenmukaista. Useampia asiakkaita koskeviin laajempiin tietoturvaloukkauksiin ilmoitusvelvollisuus pääsääntöisesti soveltuu. Näissä tilanteissa on tarpeen saada viranomaiselta ohjausta, jotta varmistetaan, että kaikki mahdollinen on tehty loukkauksen vaikutusten minimoimiseksi.

Sopimussuhteisiin liittyviä haasteita

Neuvottelut tietojenkäsittelyliitteistä ovat välillä olleet haasteellisia, kun yleisiä linjauksia esim. vastuunrajoituksista ei ole vielä muodostunut. Asiaa neuvotteluissa helpottaisi esimerkiksi valmiit mallisopimukset (vrt. komission tietojen siirtoihin liittyvät mallilausekkeet). Rekisterinpitäjä-käsittelijäsuhteiden sopiminen on ollut haastavaa erityisesti vastuiden osalta varsinkin käsittelijän kannalta.

Ongelmia on liittynyt lisäksi viranomaisten kanssa solmittuihin sopimuksiin, jossa viranomainen ei ole suostunut yksityisen toimijan kanssa tavanomaisiin sopimusjärjestelyihin tietojen käsittelystä. Esimerkkinä tästä on verottajan ylläpitämä tulorekisteri, jossa tiedon oikeellisuuden selvittäminen voi pahimmillaan jäädä taka-alalle, koska tulorekisterin vastuusuhteita ei ole määritelty riittävällä tasolla tulorekisterin käyttöehdoissa tai asiaa koskevissa sopimuksissa. Samoja ongelmia saattaa todennäköisesti liittyä parhaillaan valmisteilla olevaan maksutilirekisteriin, jossa rekisterinpitäjänä toimii Tulli.

Sisäänrakennetun tietosuojan vaatimusten sekä rekisteröityjen oikeuksien huomioiminen vanhoissa tietojärjestelmissä on osoittautunut välillä haasteelliseksi. IT-toimittajat eivät ole ottaneet asetuksen vaatimuksia tarpeeksi huomioon.

Rekisteröityjen oikeudet

Toimijat olettivat tarkastuspyyntöjen merkittävästi lisääntyvän tietosuoja-asetuksen voimaantulon yhteydessä, koska julkisuudessa tarkastusoikeutta käsiteltiin laajasti eri medioissa. Tarkastuspyynnöt lisääntyivätkin, mutta eivät kuitenkaan niin paljon kuin optimistisimmat arviot ennustivat. Tarkastuspyynnöt ovat kuitenkin viime aikoina vähentyneet jo lähes ennen asetusta olleeseen tasoon.

Finanssialan toimijoiden kokemuksen mukaan tarkastuspyynnön taustalla on usein kielteinen päätös tai muu pettymys tarjottuun palveluun. Tarkastuspyyntö ei siten näissä tapauksissa yleensä aiheudu huolesta omien henkilötietojen käsittelyyn, vaan asiakkaan kokemasta mielipahasta ja halusta aiheuttaa yritykselle lisävaivaa asiassa. Koska finanssialan toimijoilla on paljon henkilötietoja asiakkaasta pitkien sopimussuhteiden ja erityislainsäädännössä määrättyjen säilytysvelvoitteiden takia, tarkastuspyynnön toteuttaminen aiheuttaa paljon työtä. Onkin tärkeää, että normaalia useammin toistuvista pyynnöistä voidaankin periä maksua.

Haasteita liittyy myös rekisteröidyn oikeuksien toteuttamiseen lakisääteisessä tehtävässä, kun kaikkia asetuksen oikeuksia ei voida asetuksen tarkoittamalla tavalla täysimääräisesti toteuttaa eikä erityislainsäädäntö kaikissa tilanteissa anna suoraa oikeutusta asetuksesta poikkeamiseksi. Näitä ovat esimerkiksi unohdetuksi tuleminen ja tietojen siirtäminen. Tämän vuoksi rekisteröidyn oikeuksien informoiminen selosteilla on välillä haasteellista.

Onko yleisen tietosuoja-asetuksen mahdollistamaa sääntelyliikkumavaraa käytetty Suomessa tarkoituksenmukaisella tavalla?

Finanssialan toimijoiden mukaan sääntelyliikkumavaraa on pääsääntöisesti käytetty tarkoituksenmukaisella tavalla. Esimerkiksi henkilötunnuksen käyttö on perusteltua laissa säädetyissä tapauksissa kuten pankki- ja vakuutustoiminnassa, koska asiakas tulee yksiselitteisesti tunnistaa.

Kansallinen sääntely on kuitenkin vasta osin valmistunut ja monia lainsäädäntöhankkeita on edelleen kesken. Nämä viivästykset aiheuttavat rekisterinpitäjille haasteita ja oikeusepävarmuutta. Esimerkkinä tästä on vakuutusalan väärinkäytösrekisterin ylläpidon oikeuttavan lainsäädännön myöhästyminen.

Kansallisessa lainsäädännössä olisi mahdollista säätää automaattisesta päätöksenteosta tarkemmin ja sallia sen käyttö suoraan lainsäädännön perusteella. Jotta sääntely ei muodostuisi digitalisaation esteeksi, tulisi tätä mahdollisuutta käyttää. Automaattiset päätökset tulisi olla sallittuja erityisesti finanssitoiminnassa siltä osin kuin ne ovat asioiden laatuun ja laajuuteen nähden tarkoituksenmukaisia, esim. tilanteissa, jossa asiasta ei käytännössä aiheudu negatiivisia seuraamuksia päätöksenteon kohteelle (esim. myönteiset päätökset). Automaattinen päätös voi olla tilanteen mukaan joko valituskelpoinen päätös tai pieni välivaihe keskellä päätösprosessia. Digitalisaation myötä prosessit ovat käytännössä yhä enemmissä määrin automatisoituja, mistä rekisteröidytkin hyötyvät päätöksenteon nopeutumisen ja inhimillisten virheiden pienenemisen myötä.

Kansallisessa sääntelyssä on päädytty siihen, että viranomaista ei koske tietosuoja-asetuksen mukaiset sanktiot. Viranomaisen jääminen sanktioinnin ulkopuolelle haittaa yksityisen toimijan ja viranomaisasemassa toimivan keskinäisiä suhteita. Esimerkiksi työeläkeyhtiön integroidessa tietojärjestelmiä tai otettaessa käyttöön yhteiskäyttöisiä järjestelmiä viranomaisten kanssa riskinoton taso voi vaihdella toimijoiden välillä sen mukaan, sovelletaanko osapuoleen tietosuoja-asetuksen sanktiosäännöksiä vaiko ei.

Sääntelyliikkumavaran käyttö ei kuitenkaan suoraan merkitse sitä, että lainsäädäntö olisi sellaisenaan sovellettavissa teknisiin ratkaisuihin ja prosesseihin ilman mittavaa viranomaiselta saatavaa lisäohjeistusta. Tästä esimerkkinä on tietoyhteiskunnan palveluihin tarvittava suostumus, jos lapsi on alle 16-vuotta.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Kansallisesti muotoutuneet tietosuojalainsäädännön ominaispiirteet ja erityisesti rekisteriliitännäinen termistö aiheuttavat vaikeuksia tietosuoja-asetuksen tulkinnan kanssa, sillä tietosuoja-asetus ei nojaudu ns. rekisteriajatteluun. Henkilötietoja ei välttämättä tallenneta rekisteriin, vaan tietoja käsitellään esimerkiksi vain reaaliaikaisesti ja/tai väliaikaisesti (mm. tietoliikenne, paikkatiedot, verkkoselailu ja verkkopalveluiden tunnistamaton käyttö) ja usein pseudonyymissä muodossa. Tästä näkökulmasta vakiintunut termi ”rekisteröity” ei välttämättä ole onnistunut asetuksen aikana.

Rekisterinpitäjän kannalta väärintulkinnan riski liittyy erityisesti siihen, että rekisterinpitäjä ei välttämättä tiedosta rooliaan varsinkaan sellaisen henkilötietojen käsittelyn osalta, jossa henkilötietoja ei varsinaisesti tallenneta tietojärjestelmiin eikä varsinkaan sellaisiin tietokantoihin, hakemistoihin tai tietorakenteisiin, joista tiedot olisivat suoraan hakuavaimilla etsittävissä tai näytettävissä. Termi rekisterinpitäjä viittaakin liian vahvasti nimenomaisesti rekisteriin eikä niinkään siihen, mitä rekisterinpitäjällä tarkoitetaan: tahoa, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Henkilötietojen käsittelyperiaatteiden soveltamisessa esiintyy useita haasteita. Ongelmia aiheuttaa esimerkiksi rajanveto 6 artiklan mukaisten lainmukaisten käsittelyperusteiden välillä, koska joskus on vaikeata erottaa, onko kyseessä sopimuksen täytäntöön paneminen vaiko oikeutettu etu. Erityisesti oikeutettu etu käsittelyperusteena tarvitsisi entistä konkreettisempaa soveltamisohjausta.

Aiemmin voimassa olleen henkilötietolain mukaan yhtenä oikeusperusteena henkilötietojen käsittelylle oli asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan. Vakuutusalan vakiintuneen tulkinnan mukaan vapaaehtoisten vakuutusten vakuutuksenottajia, vakuutettuja, korvauksenhakijoita ja edunsaajia koskevien henkilötietojen käsittely on perustunut asiakassuhteeseen henkilötietolain nojalla ja täyttänyt yhteysvaatimuksen. Vakuutussopimuksen luonteesta ja vakuutussalaisuudesta johtuen on voitu katsoa, että vakuutettujen ja edunsaajien henkilötietoja on voitu laillisesti käsitellä silloinkin, kun nämä henkilöt eivät itse tiedä olevansa osallisina vakuutussopimuksessa. Tätä oikeusperustetta ei ole voimassa olevassa tietosuojalaissa. Siksi vakuutusyhtiöiden toimintaa koskevassa lainsäädännössä olisi täsmennettävä, mikä on oikeudellinen peruste edunsaajien ja vakuutettujen tietojen käsittelylle. Kyse ei ole aina vakuutettujen terveystiedoista, vastuuvalinnasta tai korvauspäätöksestä, joista on säädetty tietosuojalain 6 §:ssä. Ehdotamme, että 6(1) e -alakohdan mukaista kansallista liikkumavaraa käytetään käsittelyperusteen säätämiseen yllä mainittuun tilanteeseen.

Toimijoiden on usein vaikeata tulkita, milloin ja missä erityistilanteissa tietojen käsittely on oikeasuhtaista ja millaisiin suojakeinoihin tulisi milloinkin turvautua. Anonyymiä tietoa ei määritellä riittävän yksiselitteisesti, minkä vuoksi yrityksen on vaikeaa arvioida esimerkiksi verkkopalveluiden käyttötiedoista, ovatko kyseessä anonyymit tai pseudonyymit tiedot, vai edellytetäänkö esimerkiksi rekisteröidyn oikeuksien toteuttamista ja missä laajuudessa. Tästä johtuen myös 11 artiklan (käsittely, joka ei edellytä tunnistamista) soveltaminen voi olla huomattavan hankalaa.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Toimitettavat tiedot (artiklat 13-14)

Asetuksen mukainen informointivelvoite sisältää muun muassa vastaanottajien tai vastaanottajaryhmien yksilöinnin. Tietosuojatyöryhmän läpinäkyvyyttä koskevien suuntaviivojen mukaan artiklan 4 (9) kohdan perusteella voidaan tulkita, että vastaanottaja voi olla rekisterinpitäjä, yhteisrekisterinpitäjä tai henkilötietojen käsittelijä. Tämä tulkinta ei ole johdettavissa asetuksen sanamuodosta. Tulkinta johtaa harhaan käsittelijöiden ja rekisterinpitäjien roolien määrittelemisessä yksittäistapauksissa. Ehdotamme, että vastaanottajat tarkoittaisivat kolmansia osapuolia, jotka ovat rekisterinpitäjiä.

Haasteellista on myös arvioida, milloin 13 ja 14 artiklan mukaiset velvoitteet on täytetty 12.1 artiklan mukaisesti eli *”tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä”.*

FINANSSIALA

Rekisteröidyn oikeus saada pääsy tietoihin (artikla 15)

Artiklan 15 osalta tarvittaisiin toimijoille ohjeistusta siitä, mitä rekisteröidyn *”oikeus saada pääsy tietoihin”* käytännössä tarkoittaa, kun tietoa ei ole selkeästi jäsennelty tai helposti saatavilla. Epäselvyyttä aiheuttaa myös vaatimus käsiteltävistä henkilötiedoista toimitettavasta kopiosta, sillä "kopioiden" toimittamiseen voi liittyä yrityssalaisuus- ja tekijänoikeusnäkökulmia. Erityisen tulkinnanvaraista on se, koska voidaan vedota pyynnön kohtuuttomuuteen tai ilmeiseen perusteettomuuteen.

Tietosuoja-asetuksen suhde muihin säännöksiin aiheuttaa myös epäselvyyttä, sillä monet säännökset velvoittavat finanssialan toimijoita toimittamaan asiakkaille tietoja säännöllisesti (esim. maksupalvelulaki). Pahimmassa tapauksessa artiklan 15 mukaisella tietopyynnöllä voidaan ”kiertää” pankin maksupalvelulain mukainen oikeus veloittaa jo aiemmin toimitettujen tietojen uudelleen toimittamisesta.

Oikeus tietojen poistamiseen (artikla 17)

Samalla kun tietoisuus omista oikeuksistaan on lisääntynyt asetuksen voimaantulon myötä, on asiakkaiden välillä vaikea ymmärtää, ettei tietoja voida aina poistaa, koska rekisterinpitäjällä on edelleen velvollisuus tai oikeus säilyttää ne. Lisäksi joskus vaaditaan nähtäviksi tietoja, joita ei ole enää tallella, koska niitä ei ole ollut velvollisuutta säilyttää. Haasteelliseksi on myös koettu automaattisten toimintojen rakentaminen järjestelmiin tietojen poistamiseksi.

Rekisteröidyn oikeus rajoittaa käsittelyä (artikla 18)

Rekisteröidyn oikeutta rajoittaa käsittelyä on äärimmäisen vaikea toteuttaa kohdan 2 vaatimusten mukaisesti, koska sopimuksia on edelleen hoidettava ja hoito on automatisoitu järjestelmien avulla. Kyseessä on ristiriita, jonka vuoksi käytännön tasolla syntyy tilanteita, jossa oikeutta rajoittaa käsittelyä ei voida toteuttaa laissa säädellyn velvoitteen noudattamisen yhteydessä ollenkaan, esimerkiksi vakuutustoiminnassa vuositiedotteen lähettäminen tai korvauksen maksaminen.

Oikeus siirtää tiedot järjestelmästä toiseen (artikla 20)

Finanssialan toimijoiden kokemuksen mukaan rekisteröidyillä ei ole ollut olennaista kiinnostusta siirto-oikeuden käyttämiseen. Myöskään yritykset eivät ole luoneet uusia palveluja, jotka hyödyntäisivät siirto-oikeuden nojalla saatavaa henkilötietoa. Kyseisellä oikeudella ei toistaiseksi ole ollut suurta käytännön merkitystä. Samaan aikaan siirto-oikeuden edellyttämien teknisten kyvykkyyksien rakentaminen on kuitenkin rekisterinpitäjille merkittävä kustannuserä. Käytännössä tietojärjestelmistä voi olla vaikea erotella rekisteröidyn toimittamia henkilötietoja tiedoista, jotka rekisterinpitäjällä hänestä on ja jotka voivat sisältää myös jotain rekisterinpitäjän tuottamaa tietoa tai analyysiä.

Rekisteröidyn oikeus vastustaa käsittelyä (artikla 21)

Vastustamisoikeuden käyttämisen edellyttämä *"henkilökohtaiseen erityiseen tilanteeseen liittyvä peruste"* on tulkinnallisesti hyvin hankala käsite, joka soveltaminen kaipaisi selventämistä.

Automatisoidut päätökset (artikla 22)

Viittaamme kohdassa 3. esitettyyn vastaukseen automatisoitujen päätösten osalta.

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

Rekisterinpitäjän vastuu (artikla 24)

Rekisterinpitäjälle on säädetty vastuu huolehtia henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä vastaavien teknisten ja organisatoristen toimenpiteiden toteuttamisesta ja tietosuojaa koskevien toimintaperiaatteiden käyttöönotosta. Asetus antaa kuitenkin rekisterinpitäjälle vapaat kädet sekä riskien arviointiin liittyen että siitä päättämiseen, millaisia suojakeinoja ja -mekanismeja rekisterinpitäjä ottaa käyttöönsä. Tämä asettaa rekisterinpitäjät pahimmillaan eriarvoiseen asemaan: kustannukset voivat valituista mekanismeista riippuen erota toisistaan merkittävästi. Koska riittävän täsmällistä ohjeistusta ei ole saatavilla, rekisterinpitäjällä ei ole mitään keinoa varmistua etukäteen, onko käytetty riskien arvioinnin mekanismi hyväksyttävä, ovatko arvioidut riskit tulkittu oikein ja ovatko suojakeinot mitoitettu oikein.

Henkilötietojen käsittelijä (artikla 28)

Säännökset rekisterinpitäjän ja henkilötietojen käsittelijän vastuunjaosta on asetusta sovellettaessa todettu erityisen epäselväksi. Asiakkaiden henkilötietoja käsitellään yhteistyössä muiden yritysten kanssa ja roolitus on asetuksen säädösten perusteella monesti tulkinnanvaraista. Epäselvyyksiä on liittynyt esimerkiksi siihen, mikä yhtiö määrittää henkilötietojen käsittelyn tarkoitukset, kun käsittely hyödyttää molempia osapuolia ja missä tilanteessa on kyse yhteisrekisterinpitäjyydestä. Asetus ei vastaa kysymykseen siitä, voiko sopimuksessa rajoittaa henkilötietojen käsittelijän vahingonkorvausvastuuta, jos käsittelijä rikkoo sopimusta tietojen käsittelystä. Tietosuojaliitteiden tuominen osaksi sopimuskokonaisuuksia on ollut vaikeaa, kun jo osapuolten keskinäisestä roolista on ollut epäselvyyttä.

Tietojen käsittelyä koskevien sopimusten laatiminen on ollut työlästä ja ainakin osittain johtunut siitä, että käsittelijöiden on ollut vaikea hahmottaa velvoitteitaan hyvin yleisellä tasolla olevan asetustekstin perusteella. Tulkinnanvaraisuutta aiheuttavat asetuksessa käytetyt termit *"asianmukaisilla toimenpiteillä"* ja *"mahdollisuuksien mukaan"*. Koska sääntelyssä ei ole selkeää suhteellisuusperiaatetta, sopimuksen laajuuden ja yksityiskohtaisuuden oikeasuhteisuuden määrittäminen kussakin sopimussuhteessa on haastavaa.

Vaikeuksia sopimusneuvotteluissa ovat aiheuttaneet niin ikään kulujen jakaantuminen erityisesti seuraavissa asioissa: rekisterinpitäjät ohjeet, rekisteröityjen oikeudet, avustus DPIA toteuttamisessa ja tietosuojaloukkauksen ilmoittamisessa sekä auditointi ja sen laajuus. IT-toimittajien palveluiden tulisi oletusarvoisesti täyttää tietosuojalainsäädännön edellytykset eikä pakottavan lainsäädännön asettamista velvoitteista tulisi periä ylimääräisiä kuluja. Asetuksessa olisi tullut velvollisuuksien asettamisen ohella säätää myös kustannusten jakaantumisesta rekisterinpitäjän ja käsittelijän välillä.

Lisäksi neuvotteluissa on havaittu epäselvyys sellaisten alihankkijoiden roolista, jotka välittävät tietoja. Tällaisia toimijoita ovat esimerkiksi sähköisiä viestintäpalveluita tarjoavat toimittajat, kuten teleoperaattorit, sähköpostipalveluntarjoajat tai

maksunvälittäjät, jotka käsittelevät tietoja yhtä paljon niin lähettäjän kuin vastaanottajankin lukuun. On epäselvää, tuleeko nämä toimijat tulkita rekisterinpitäjiksi, käsittelijöiksi vai kolmansiksi osapuoliksi ja kuinka vastuuasetelmat tulisi tällaisessa tilanteessa jäsentää.

Alihankintaketjun selvittämisvelvoitteen toteuttamiseen liittyy haasteita. Käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia. Muutoksesta sopiminen on kuitenkin näissä tilanteissa haastavaa. Lisäksi on vaikeaa arvioida, missä laajuudessa rekisterinpitäjän pitäisi ulottaa valvontatoimenpiteitä henkilötietojen käsittelijään jatkuvassa toiminnassa.

Käsittelyn turvallisuus (artikla 32)

Tietoturvavaatimukset eivät sisällä yksiselitteisiä vaatimuksia toimialoittain. Riskienarviointi suhteessa tietoturvatoimiin kriteerinä jättää paljon harkinnanvaraa, eikä ole olemassa objektiivisia mittaamiskeinoja tarvittaville toimille. Asiassa tulisi olla selkeät määrittelytavat sille, millä tavalla uusin tekniikka ja toteuttamiskustannukset tulee ottaa huomioon riittävän tietosuojan toteuttamiseksi, jotta voidaan määrittää tarvittavat tietoturvatoimenpiteet tietynlaisille henkilötietojen käsittelylle.

Tietoturvaloukkauksista ilmoittaminen (artikla 33)

Henkilötietojen tietoturvaloukkauksien osalta viranomaisilmoituksen 72 tunnin aikaraja aiheuttaa haasteita sekä myös lisää yritysten kustannuksia (mm. ylityöt, päivystykset) sekä vie erityisesti pienemmissä organisaatioissa resursseja ja aikaa itse tilanteen selvittämiseltä ja korjaamiselta.

Tietoturvaloukkauksissa käytettävä ilmoituslomake ei ole käyttäjäystävällinen eikä palvele esimerkiksi lisätietojen antamista aiempaan ilmoitukseen. Ongelmallisena on pidetty myös sitä, että viranomaisen päätökset ja muut vastaukset ilmoituksiin annetaan useiden kuukausien viiveellä. Finanssialan toimijoiden näkemyksen mukaan ajantasaista viranomaisohjausta poikkeamatilanteiden käsittelyyn tai linjausten tekemiseen poikkeamatilanteen päällä ollessa ei ole ollut riittävästi saatavilla.

Viittaamme lisäksi kohdassa 2 annettuun vastaukseen.

Tietosuojaa koskeva vaikutustenarviointi (artikla 35)

Viranomaislinjausten ja -ohjeiden vähäisyys riskiarviointien tekemisessä sekä ilmoitusvelvollisuuden ja ilmoituskynnysten ylittymisen arvioimisessa aiheuttaa eriäviä käytäntöjä organisaatioissa. Euroopan tietosuojaviranomaisten tulisi määritellä tietosuojan vaikutustenarviointien yleiset sisältö- ja muotovaatimukset niin tarkalla tasolla, että kaikki voisivat tehdä ne samalla perusmallilla. Nyt on epäselvyyttä siitä, mikä on riittävä taso. Artiklan kohdissa 4 ja 5 valvontaviranomaisille annettu mahdollisuus luoda luetteloita on johtanut eri maissa erilaisten luetteloiden julkaisemiseen. Luetteloiden yhdenmukaisuudesta tulisi huolehtia EU-tasolla.

Tietosuojavastaavan asema ja tehtävät (artiklat 38 ja 39)

Tietosuojavastaavan tehtävät ovat hyvin laajoja, kuten esimerkiksi velvoite ottaa tietosuojavastaava mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Sellaisilla liiketointa-alueilla, jotka perustuvat henkilötietojen käsittelyyn kuten finanssiala, on tietosuojavastaava käytännössä otettava mukaan lähes kaikkiin asioihin.

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

Tyypillisin finanssialalla käytetty siirtomekanismi on ollut EU:n mallisopimuslausekkeet, joita pidetään pääsääntöisesti toimivina ja ne koetaan hyödylliseksi, sillä niiden käyttäminen säästää aikaa ja ne tuovat turvaa etenkin pienemmille toimijoille.

Henkilötietojen siirtoa käsittelevä luku ei kuitenkaan tarjoa vastausta siihen, tuleeko palvelun käyttöä tulkita siirroksi. Digitaaliset palvelut edellyttävät ulkoisten palveluntarjoajien käyttöä ympäri vuorokauden ja globaalissa taloudessa toimiakseen digitaalisten palveluiden tulee muodostua moninaisista, skaalautuvista alihankintaketjuista. Tällöin palveluiden toimivuus ja ylläpito myös edellyttävät, että ylläpitopalvelua tuotetaan kolmansista maista. Alkuperäisen rekisterinpitäjän on välillä haastavaa saada täysi käsitys siitä, ketkä ovat käsittelemässä tietyn rekisteröidyn tietoja.

Epäselvyyttä on aiheuttanut myös merkittävässä markkina-asemassa olevien pilvipalveluntarjoajien globaali toiminta. Tällaisten palveluntarjoajien asiakkaana olevat rekisterinpitäjät eivät tosiasiallisesti pysty vaikuttamaan tietojen käsittelyyn. Tästä syystä nämä globaalit toimittajat tulisi tulkita rekisterinpitäjiksi ja saada vastuuseen tietojen käsittelyn tarkoituksista ja keinoista.

Kommentit yleisen tietosuoja-asetuksen VI lukuun – Riippumattomat valvontaviranomaiset

Tietosuojaviranomaisten toiminta tulee riittävästi resursoitu, jotta viranomaisilla olisi paremmin aikaa tehdä yhteistyötä eri toimialojen edustajien kanssa ja antaa toimialakohtaisia neuvoja ja avustaa asetuksen tulkinnassa. Ohjeistusta annettaessa tulee ottaa huomioon toimialakohtaiset erityispiirteet.

Valtuutetun nettisivujen informaatiota pidetään selkeänä ja asiallisena, mutta osana hyvää hallintoa viranomaisen tulisi aktiivisesti tiedottaa sivulla tehdyistä muutoksista.

Finanssialan yrityksillä ei ole vielä kokemuksia Finanssivalvonnan valvonnasta tietosuoja-asioissa.

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

Rahanpesulain asiakkaan tuntemista ja tietojen säilyttämistä koskevien säännösten ja tietosuojasäännösten yhteensovittamisessa on haasteita, minkä selkeyttämiseksi tarvittaisiin yhteistyötä asianomaisten viranomaisten kanssa. Esimerkkeinä voidaan mainita USA:n OFAC-pakotelistausten seuraaminen ja niiden käyttäminen monitoroinnissa tai ”adverse median” eli kielteisen mediajulkisuuden käyttäminen asiakkaan tuntemisessa.

Myös petosten torjunnassa kysymyksiä on herättänyt se, onko mahdollista vaihtaa tietoja pankkitilin numerosta tai voiko vakuutusyhtiö varmistua siitä, kenelle ilmoitettu tilinumero kuuluu. Samoin IP-osoitteen käyttöön petostentorjunnassa liittyy eriäviä näkemyksiä. Rahanpesun ja petosten estämiseen liittyvistä toimenpiteistä ja niiden oikeusperustasta pitäisi ehdottomasti säätää erityislainsäädännössä, eikä finanssialan toimijoiden pitäisi joutua itse ratkaisemaan sitä, miten osittain ristiriitaisia säännöksiä tulee noudattaa.

Finanssialan yrityksillä ei ole vielä kokemuksia Tietosuojavaltuutetun toimiston ja Finanssivalvonnan yhteistyön toimivuudesta.

Tietosuoja-asetuksessa ei ole lainvalintasäännöksiä. Kansalliset lainvalintasäännökset voivat sen sijaan olla ristiriitaisia. Kansainvälisesti toimiville yrityksille (esimerkiksi sivuliikkeiden kautta) on epävarmaa, minkä maan tietosuoja-asetusta täydentävää kansallista lakia tulee soveltaa.

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

Asetus on paikon tulkinnanvarainen ja sen asettamat velvoitteet ovat periaatetasolla, joten arviointia asetuksen vaatimusten noudattamisesta on hankalaa mitata. Ankaran vastuun asettaminen ja käännetty todistustaakka puolestaan edellyttävät oikeusvarmuutta. Merkittävien sanktioiden asettaminen yrityksille tilanteessa, jossa rekisteröidylle ei aiheudu vahinkoa, on vastoin EU:n yleisiä oikeusperiaatteita, kuten suhteellisuusperiaatetta. Viranomaisten käyttämät valtuudet tulee suhteuttaa asetuksen tulkinnanvaraisuuteen, minkä vuoksi olisi toivottavaa, ettei valvontaviranomainen lähtisi asetuksen seuraamusten osalta käyttämään ensi sijassa sanktioita. Tarvittavat muutokset käytäntöihin on saatavissa ohjaamalla toimintaa huomautuksilla viranomaisen tulkinnan mukaiseen suuntaan.

Asiantuntijalautakuntaan tulisi nimittää rekisterinpitäjien edustajia oikeusvarmuuden turvaamiseksi. Tällöin toimialakohtaiset ratkaisut tulisivat arvioitaviksi ja olisi toivottavaa, ulkopuolisten asiantuntijoiden lausunto pyydetään aina päätettäessä merkittävistä sanktioista tietylle yritykselle tai viranomaisen ohjeistuksesta, kuten esimerkiksi päätettäessä luetteloa käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi.

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

Ei kommentteja.

FINANSSIALA RY

Lea Mäntyniemi