VN/23585/2023

Oikeusministeriön lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Valtiovarainministeriön lausunto:

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

Euroopan unionin yleisellä tietosuoja-asetuksella (EU) 2016/679 on ollut merkittävä vaikutus henkilötietojen käsittelyyn ja sen periaatteisiin Euroopassa ja myös globaalisti. Asetuksen soveltamisella on ollut useita hyötyjä ja se on yleisesti ottaen parantanut henkilötietojen suojan tasoa. Asetusta on toisaalta perustellusti myös kritisoitu.

Tietoon ja sen hyödyntämiseen panostavissa yhteiskunnissa teknologinen kehitys ja innovaatiot ovat keskeisessä asemassa ihmisten hyvinvoinnin parantamiseksi ja niukkojen resurssien parhaalla tavalla hyödyntämiseksi. Tietosuoja-asetuksen asettamien henkilötietojen käsittelyn tiukkojen reunaehtojen on kuitenkin usein koettu hidastavan tällaista kehitystä. Esimerkiksi asetuksen mukainen henkilötiedon käsitteen määritelmä, sen tulkinnat ja siten asetuksen soveltamisalan laajuus toimivat usein teknologisen kehityksen ja digitalisaation esteenä. Tietosuoja-asetuksen soveltamisalaan on katsottu kuuluvan laajasti sellaisiakin tietoja, joista luonnollisen henkilön tunnistaminen on hyvin epätodennäköistä ja vaatisi useita muitakin tietoja. Kun tällaisetkin tiedot katsotaan henkilötiedoiksi, on niiden käsittelyn täytettävä tietosuoja-asetuksen edellytykset, jotka ovat esimerkiksi tietojensiirtojen osalta hyvin korkeat. Tällä tavoin tietosuoja-asetuksen soveltamisala kasvaa perusteettoman laajaksi.

Nykyaikaisten teknologioiden, kuten pilvi- ja tekoälyratkaisujen laajamittaisen hyödyntämisen kannalta olisi tärkeää, että tietosuoja-asetuksen henkilötiedoksi katsottavien tietojen alaa rajattaisiin. Kun esimerkiksi tietoja siirretään pilvipalveluun, siirtyy samalla usein myös diagnostiikkatietoja ja epäsuoria tunnistetietoja tietojen tallentajasta, rekisteröijästä tai muusta vastaavasta luonnollisesta henkilöstä. Pilvipalvelujen käytön kannalta on ongelmallista, mikäli tällaiset hyvin hypoteettisesti tunnistettavaan henkilöön liittyvät tiedot, kuten dynaamiset IP-osoitteet katsotaan henkilötiedoiksi, sillä tällöin niiden siirtämiselle julkiseen globaaliin pilvipalveluun on oltava tietosuoja-asetuksen V luvun mukainen siirtoperuste. Näin on erityisesti nykyisenkaltaisessa tilanteessa, jossa tietosuoja-asetuksen 45 artiklan mukaisten Euroopan komission antamien tietosuojan riittävyyttä koskevien, niin sanottujen vastaavuuspäätösten hyödyntämiseen henkilötietojen siirtoperusteena liittyy epävarmuustekijöitä.

Tietosuoja-asetuksen johdanto-osan 26 kohdassa todetaan, ettei asetus koske anonyymien tietojen käsittelyä. Asetus kuitenkin koskee pseudonymisoituja henkilötietoja, eli tietoja, jotka voidaan yhdistää luonnolliseen henkilöön lisätietoja käyttämällä. Tämä jaottelu onkin vahvana lähtökohtana, eikä asetus kovin hyvin mahdollista esimerkiksi henkilötietojen käsittelyä tai siirtoa niiden salaamisen perusteella, sillä tällöin rekisterinpitäjän on mahdollista esimerkiksi salausavaimen avulla palauttaa tiedot

tunnisteellisiksi. Digikehitystä edistäisi, mikäli hyvin teoreettisesti yksittäiseen henkilöön liittyviä tietoja tai koodattuja tai salattuja henkilötietoja, joiden tunnistettavaksi palauttaminen on mahdollista ainoastaan rekisterinpitäjälle itselleen, voitaisiin nykyistä laajemmin tulkita anonymisoiduiksi. Tällöin rekisterinpitäjät voisivat tiedot salaamalla siirtää henkilötietoja pilvipalveluihin ja samalla huolehtia siitä, että rekisteröityjen henkilötietojen suoja ei vaarannu siirron johdosta.

Tietosuoja-asetus on nähty julkisessa hallinnossa laajasti pilvipalveluiden hyödyntämisen hidasteena. Tämä on kestämätöntä tilanteessa, jossa julkiselta hallinnolta ja sen digipalveluilta edellytetään yhä suurempaa tehokkuutta, sujuvuutta, käyttövarmuutta ja turvallisuutta. Pilvipalveluille ominaisia etuja ovat juurikin skaalautumiskyky, muuntautumiskykyisyys, joustavuus ja innovatiivisuus. Pilvipalveluilla on pystytty saavuttamaan taloudellista hyötyä sekä saatu parannettua tietoturvallisuutta. Pilvipalveluteknologiat on huomioitava palveluja kehitettäessä ja suunniteltaessa ja monissa tilanteissa pilvipalvelu onkin jatkossa ainoa mahdollinen palvelumalli. Julkishallinnon on vääjäämättä siirryttävä laajemmin hyödyntämään pilvipalveluita huolehtiakseen siitä, että se pystyy tarjoamaan nykyaikaisia digipalveluja ja samalla huolehtimaan niihin liittyvistä turvallisuusriskeistä. Tietojärjestelmien kehittämisratkaisut tehdään pitkällä tähtäimellä, mihin henkilötietojen käsittelyyn ja siirtämiseen liittyvä epävarmuus sopii huonosti. Mikäli henkilötietojen käsitteen ala olisi rajatumpi tai niiden siirtoperusteet vakiintuneemmat, olisi sillä merkittävä vaikutus julkishallinnon pilvisiirtymän ja myös muun digikehityksen tehokkuuden kannalta.

Tietosuoja-asetuksen 5 artiklan mukaisista henkilötietojen käsittelyä koskevista periaatteista erityisesti käyttötarkoitussidonnaisuuden periaate on myös nähty haasteena julkisen hallinnon digitalisaatiokehitykselle. Uusien digitaalisten palvelujen ja tietojärjestelmien käyttöönotossa on toimivuuden varmistamiseksi lähes aina viimeistään testauksen loppuvaiheissa oltava mahdollisuus käyttää niin sanottua aitoa tuotantodataa, johon useimmiten sisältyy myös henkilötietoja. Rekisterinpitäjät kuitenkin keräävät rekisteröityjen henkilötietoja muuta tarkoitusta kuin tietojärjestelmien kehittämistä tai testaamista varten, jolloin henkilötietojen käsittely esimerkiksi järjestelmää testatessa merkitsee lähtökohtaisesti poikkeusta käyttötarkoitussidonnaisuuden periaatteeseen. Digikehityksen ja esimerkiksi tekoäly- ja pilvisiirtymän edistämisen näkökulmasta olisi hyödyllistä, mikäli jo asetustasolla mahdollistettaisiin rajatuissa määrin henkilötietojen käsittely teknologian kehittämistarkoituksessa.

Tietosuoja-asetuksen johdanto-osan 4 kohdassa on mainittu, että henkilötietojen käsittely on suunniteltava ihmistä palvelevaksi ja että oikeus henkilötietojen suojaan ei ole absoluuttinen vaan sitä on tarkasteltava suhteessa sen tehtävään yhteiskunnassa ja sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin. Tietosuoja-asetuksen soveltamisessa on havaittu ongelmia tämän suhteellisuusperiaatteen toteutumisessa. Asetuksen henkilötietojen käsittelylle asettamat tiukat reunaehdot ja niiden tiukka tulkintatapa korostavat henkilötietojen suojaa silloinkin, kun se ei olisi tarkoituksenmukaista eli esimerkiksi silloin, kun käsiteltävien henkilötietojen määrä, luonne, tietojen suojaaminen, pseudonymisointi ja muut seikat yhdessä tekevät ilmeiseksi sen, että rekisteröidyn oikeuksille ja vapauksille ei aiheudu käsittelyn johdosta tosiasiallista riskiä. Esimerkiksi erilaisten uusien teknologioiden käyttöönotolla pyritään useimmiten tarjoamaan asiakkaille parempia, tehokkaampia ja paremmin suunnattuja palveluja, siis palvelemaan kansalaista. Rekisterinpitäjät ovat kuitenkin monesti kokeneet

tietosuoja-asetuksen estävän tällaistakin henkilötietojen käsittelyä edellyttävää kehittämistä, mitä ei voida pitää asetuksenkaan tarkoituksen mukaisena.

Tietyissä tilanteissa haasteena on ollut myös tietosuoja-asetuksen soveltamiseen liittyvän yleisen tulkinta- ja oikeuskäytännön puuttuminen suhteessa tietosuoja-asetuksessa osin melko yleisellä tasolla säädettyihin henkilötietojen käsittelyn periaatteisiin. Tästä on aiheutunut jonkin verran tulkinta- ja rajanveto-ongelmia sen suhteen, millaisia rekisterinpitäjän toteuttamia teknis-toiminnallisia ratkaisuja on voitu pitää tietosuoja-asetuksen puitteissa mahdollisina tai hyväksyttävinä. Konkreettisena esimerkkinä voidaan mainita esimerkiksi asetuksen 5 artiklan 1d alakohdan säännökset suhteessa siihen, milloin rekisterinpitäjän käytännössä voidaan katsoa toteuttaneen kaikki *kohtuulliset* toimenpiteet epätarkkojen tai virheellisten henkilötietojen poistamiseksi tai korjaamiseksi ja toisaalta millaisia toimenpiteitä ei voida enää pitää sellaisina, joita rekisterinpitäjältä *kohtuudella* voitaisiin edellyttää.

Toisaalta myös kansallisen valvontaviranomaisen asetuksen soveltamiseen liittyvät tulkintalinjaukset ovat eräillä osa-alueilla tiukentuneet tietosuoja-asetuksen voimassaoloaikana, jolloin kansallisessa lainsäädännössä valittuja alun perin hyväksyttäviksi oletettuja sääntelyratkaisuja joudutaan tietosuoja-asetuksen vastaisina myöhemmin muuttamaan. Esimerkkinä voidaan mainita tulotietojärjestelmästä annetun lain 4 §:n säännökset rekisterissä olevien tietojen oikeellisuuteen liittyvistä vastuista, joiden sisältöön valvontaviranomainen ei HE:n 134/2017 eduskuntakäsittelyn yhteydessä kiinnittänyt erityistä huomioita tietosuoja-asetuksen näkökulmasta, mutta jotka sittemmin on katsottu tietosuoja-asetuksen vastaisiksi kansallisen sääntelyliikkumavaran puuttumisen vuoksi.

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

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?

Tietosuoja-asetuksen sääntelyliikkumavara ei lopulta ole kovinkaan laaja. Asetus kuitenkin jättää osin kansallisesti mahdolliseksi säätää niistä tarkoituksista, joissa henkilötietojen käsittely on sallittua. Tietosuoja-asetuksen johdanto-osan 50 kohdassa on mainittu, että kansallisesti on mahdollista säätää niistä yleisistä eduista, tehtävistä ja tarkoituksista, joissa myöhempää henkilötietojen käsittelyä muussa kuin alkuperäisessä käsittelytarkoituksessa olisi pidettävä yhteensopivana ja laillisena. Tietosuojalain (1050/2018) 4 §:ssä tätä sääntelyliikkumavaraa on käytetty, kun on säädetty tilanteista, joissa henkilötietojen käsittely on mahdollista tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdassa tarkoitetun yleistä etua koskevan tehtävän suorittamisen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämisen mukaisesti. Vaikka erityisesti tietosuojalain 4 §:n 1 momentin 2 kohtaa on käytetty julkishallinnossa kehittämistyössä henkilötietojen käsittelyn perusteena, olisi teknologian kehittämisen ja digitalisaation kannalta selkeämpää, mikäli viranomaisten suorittama henkilötietojen käsittely tällaisiin tarkoituksiin olisi nykyistä suoremmin mahdollistettu. Tämä yhdenmukaistaisi eri viranomaisten mahdollisuuksia henkilötietojen käsittelyyn digitalisaation

edistämistarkoituksissa sekä parantaisi niiden mahdollisuuksia informoida rekisteröityjä tällaisesta henkilötietojen käsittelystä. Tällainen sääntely voisi olla perusteltua lisätä yleislakiin, eikä eri viranomaisia koskeviin erityislakeihin.

Tietosuoja-asetus mahdollistaa rajatusti myös henkilötietojen siirtoja koskevan kansallisen sääntelyn antamisen. Tietosuoja-asetuksen 49 artiklassa on säädetty erityistilanteita koskevista poikkeuksista, joiden perusteella henkilötietojen siirrot voidaan oikeuttaa silloin kun muut asetuksen V luvussa mainituista siirtoperusteista eivät sovellu. Artiklan 1 kohdan d alakohdassa on säädetty mahdollisuudesta tietojen siirtämiselle, jos se on tarpeen tärkeää yleistä etua koskevien syiden vuoksi. Tämän siirtoperusteen käyttäminen edellyttää 49 artiklan 4 kohdan mukaisesti sitä, että kyseessä oleva yleinen etu on tunnustettu unionin oikeudessa tai kansallisessa lainsäädännössä. Näin ollen olisikin hyödyllistä, mikäli kansallisesti esimerkiksi juurikin tietosuojalaissa säädettäisiin erikseen niistä tärkeistä yleisistä eduista, joiden perusteella 49 artiklan 1 kohdan d alakohdan mukaisia henkilötietojen siirtoja voitaisiin suorittaa. Tällöin rekisterinpitäjillä olisi viimesijaisena henkilötietojen siirtojen perusteena mahdollista käyttää asetuksen 49 artiklan mukaista erityistilanteita koskevaa poikkeusta.

Rajatun käsittelyn ja henkilötietojen siirtämisen teknologian kehittämistarkoituksessa nykyistä paremmin mahdollistavat muutokset tietosuojalakiin olisivat näin omiaan edistämään suomalaisen yhteiskunnan pilvisiirtymää, jonka tavoitteena on varmistaa se, ettemme jää kehityksessä muista yhteiskunnista jälkeen.

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?

Julkishallinnon tietojärjestelmä- ja digitalisaatiokehitys toteutetaan usein julkisten hankintojen kautta. Erityisesti yhteishankintana toteutettavissa hankinnoissa rekisterinpitäjien on ollut hankalaa toteuttaa tietosuoja-asetuksen heille asettamia velvollisuuksia. Mikäli esimerkiksi julkishallinnon yhteishankintayksikkö Hansel on toteuttanut kilpailutuksen, eivät rekisterinpitäjät ole aina voineet täysimääräisesti vaikuttaa laadittavien sopimusten henkilötietojen käsittelyä koskeviin liitteisiin. Hankintasääntelyn ja tietosuoja-asetuksen yhteensovittamistarpeita olisikin syytä tarkastella ja toteuttaa mahdollisesti tarvittavat lakimuutokset tai laatia aiheeseen liittyvää ohjeistusta kansallisesti tai Euroopan tietosuojaneuvoston toimesta.

Jonkin verran haasteita on liittynyt myös kansallisen sääntelyliikkumavaran puuttumiseen tiettyjen asetuksen 5 artiklan rekisterinpitäjälle osoittamien henkilötietojen käsittelyyn liittyvien vaatimusten osalta. Esimerkkinä tästä voi mainita sen, että henkilörekistereissä olevien tietojen oikeellisuuteen liittyviä vastuita ei voida säätää miltään osin muun kuin rekisterinpitäjän itsensä hoidettavaksi ilman, että kyseinen toinen osapuoli samalla muuttuu vähintäänkin asetuksen tarkoittamaksi yhteisrekisterinpitäjäksi. Esimerkiksi tulorekisterin ja positiivisen luottotietorekisterin kohdalla vastuun rekisterissä olevien tietojen oikeellisuudesta voisi tiettävästi helpoimmin kantaa muu taho kuin rekisterinpitäjä

itse. Kuitenkaan tätä toista osapuolta – kuten työnantajaa tai luottolaitosta – ei ole katsottu voitavan saattaa yhteisrekisterinpitäjän asemaan yhdessä viranomaisen kanssa sen vuoksi, että kyse on yksityisen sektorin toimijasta, mikä kuitenkin tietosuoja-asetuksen perusteella olisi ainoa mahdollinen vaihtoehtoinen ratkaisu asiassa. Tämän seurauksena asetuksen 5 artiklassa säädettyihin rekisterinpitäjän vastuisiin kytkeytyvä kokonaisuus voi tiettyyn tapaukseen liittyvien kansallisten erityispiirteiden johdosta muodostua pakotetusti epätarkoituksenmukaiseksi sekä rekisterinpitäjän itsensä, että myös rekisteröidyn omien oikeuksien toteutumisen näkökulmasta. Tietosuoja-asetuksen mukaista kansallista sääntelyliikkumavaraa voisikin olla syytä jossain määrin laajentaa nykyisestä siten, että asetuksessa mahdollistettaisiin kansallisessa lainsäädännössä perustellusta syystä tehtävät poikkeukset ainakin tiettyjen asetuksen 5 artiklan rekisterinpitäjään itseensä kohdistamien vaatimusten osalta.

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

Jäsenvaltioiden keskenään erilaisesta sääntelystä ja tietosuoja-asetuksen erilaisista tulkinnoista seuraa se, ettei henkilötietojen suojan taso toteudu täysin yhteismitallisena eri jäsenvaltioissa. Nämä sääntelyn ja tulkintojen eroavaisuudet näkyvät muun muassa eroissa jäsenvaltioiden digitaalisessa infrastruktuurissa ja uusien teknologioiden hyödyntämisessä. Esimerkiksi Hollannissa julkinen sektori on katsonut laajemmin voivansa hyväksyä globaalien palveluntarjoajien julkisten pilvipalveluratkaisujen käytön myös henkilötietojen käsittelyssä, kun taas Suomessa on usein arvioitu, että pilvipalveluntarjoajien hyväksymät henkilötietojen käsittelyehdot eivät täytä tietosuoja-asetuksen vaatimuksia. Tietosuoja-asetuksen henkilötietojen siirtoja koskevia säännöksiä tulisikin täsmentää siten, että tällaiset jäsenvaltioiden väliset erot henkilötietojen käsittelyn keskeisten ratkaisujen osalta eivät olisi mahdollisia.

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

Euroopan tietosuojaneuvoston ohjeet antavat suuntaviivoja asetuksen eri osien tulkintaan ja niistä on ollut hyötyä käytännön soveltamistilanteissa. Asetuksen tavoin myös tietosuojaneuvoston ohjeet ovat kuitenkin osin vaikeaselkoisia ja tulkinnanvaraisia. Lopullisen harkinnan jäädessä rekisterinpitäjille eroavat eri organisaatioiden toimintatavat asetuksen vaatimusten toteuttamisessa merkittävästikin toisistaan. Julkisen hallinnon kokonaisvaltaisen digikehityksen kannalta tietosuojaneuvoston ohjeiden tulisi vakiinnuttaa tilannetta ja antaa rekisterinpitäjille lopullinen varmuus tulkinnan oikeellisuudesta. Jokaista tulkintatilannetta ei tietenkään voida huomioida ohjeissa, mutta nykyisissä ohjeissa olisi jonkin verran täsmennysvaraa, esimerkiksi henkilötietojen siirtojen osalta.

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?

Organisaatiomme ei ole ollut mukana käytännesääntöjen laatimisessa.

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

Asetuksen täytäntöönpanoon liittyvä seuraamusjärjestelmä nähdään yleisesti ottaen nykyisellään tarkoituksenmukaisena eikä erityisiä siihen liittyviä haasteita ole tunnistettu. Valtiovarainministeriö ei myöskään näe tarpeelliseksi tietosuojalain 27 § 4 momentin muuttamista siten, että seuraamusmaksua voitaisiin määrätä myös momentissa tarkoitetuille viranomaistoimijoille.

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?

Globalisoituvassa digitaalisessa maailmassa tietosuoja-asetuksen V luvun lähtökohtaa siitä, että tietojen siirtäminen kolmansiin maihin tai kansainvälisille järjestöille on mahdollista vain V luvussa mainituilla henkilötietojen siirtoperusteilla, on koettu haastavaksi toteuttaa. Näin on erityisesti, kun huomioidaan henkilötiedon käsitteen ja siten myös asetuksen soveltamisalan laajuus. Erityisen haastavaa tämä on pilviratkaisuihin pohjautuvien teknologioiden hyödyntämisessä. Suurimmat ja merkittävimmät pilvipalveluntarjoajat toimivat Yhdysvalloissa, johon suuntautuvilla henkilötietojen siirroilla ei ole ollut vakaata oikeudellista perustaa.

Euroopan komission heinäkuussa 2023 antama Yhdysvaltain riittävää tietosuojan tasoa koskeva päätös on merkittävä julkisen hallinnon pilvisiirtymää edistävä tekijä. Vastaavuuspäätöksen nojalla henkilötietoja voidaan tietosuoja-asetuksen 45 artiklan mukaisesti siirtää sertifioituneille yhdysvaltalaiselle yritykselle, jotka ovat sitoutuneet EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä sovittuihin suojatoimiin. Vastaavuuspäätöstä onkin siirtoperusteiden etusijajärjestyksen mukaisesti jatkossa käytettävä ensisijaisena henkilötietojen siirtoperusteena.

On kuitenkin todennäköistä, että aiempien Safe Harbor- ja Privacy Shield -järjestelyjen tavoin myös uusi EU:n ja Yhdysvaltojen välinen tietosuojakehys haastetaan oikeuskäytännössä. Rekisterinpitäjien kannalta esimerkiksi pilvisiirtymän edistäminen ja henkilötietojen siirtäminen vastaavuuspäätöksen nojalla on siis edelleen osin epävarmalla pohjalla. Tietojärjestelmä- ja muu kehitystyö julkishallinnossa edellyttää pitkäjänteistä suunnittelua, jollaisen edellytyksiä henkilötietojen käsittelyn sääntelyyn liittyvät epävarmuudet ymmärrettävästi heikentävät. Tietosuoja-asetuksen tulisi digikehityksen ja pilvisiirtymän näkökulmasta mahdollistaa nykyistä laajemmin tietojen siirtäminen Yhdysvaltoihin vastaavuuspäätöksen lisäksi muillakin siirtovälineillä siltä varalta, että uusikin tietosuojakehys todettaisiin myöhemmin pätemättömäksi.

Pilvipalvelujen käyttöä julkishallinnossa edistäisi, mikäli henkilötietojen siirtoja voitaisiin nykyistä laajemmin toteuttaa rekisterinpitäjien riskiperusteisiin arvioihin perustuen. Tällä tarkoitetaan sitä, että mikäli siirrettävien henkilötietojen määrä, luonne, tietojen suojaaminen ja muut seikat yhdessä tekevät ilmeiseksi sen, että rekisteröidyn oikeuksille ja vapauksille ei aiheudu riskiä siirron johdosta, voisi tiedot siirtää myös ilman erityistä siirtoperustetta. Mikäli jäännösriski saadaan minimoitua siten, että riskin aiheutuminen on epätodennäköistä, tulisi sen riittää tietojen siirtämisen perusteeksi. Tällä tavoin

pilviratkaisujen käyttöönoton mahdollisuudet kevenisivät merkittävästi, sillä käyttöönoton haasteena usein koetaan olevan juurikin henkilötietojen siirtoa koskevat säännökset. Näin on, vaikka siirrettävät henkilötiedot olisivat minimoituja ja esimerkiksi salattuja tai pseudonymisoituja, jolloin rekisteröidylle aiheutuvien riskien todennäköisyys on varsin spekulatiivisella tasolla. Selkeämpi malli, jolla henkilötietoja voidaan siirtää myös julkisiin globaaleihin pilviympäristöihin silloin kun käsittelyyn liittyvien riskien minimoinnista on huolehdittu, edistäisi merkittävästi nykyistä tilannetta, jossa tulkinnat pilvipalvelujen käytöstä vaihtelevat merkittävästi.

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?

Tiedossamme ei ole, että laajennettua alueellista soveltamisalaa koskeva sääntely ei olisi toiminut tarkoituksenmukaisella tai toivotulla tavalla. Asetuksen täytäntöönpanoon liittyvään yhteistyöhön kolmansien valtioiden kanssa valtiovarainministeriöllä ei ole kommentoitavaa.

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Tietosuoja-asetuksen 4 (1) artiklan 1 kohdan mukainen henkilötiedon käsite on varsin laaja, kun henkilötietoja ovat myös sellaiset tiedot, joista rekisteröity on epäsuorasti tunnistettavissa. Määritelmä on myös tulkinnanvarainen ja sitä on käytännössä tulkittu laajentavaan tapaan. Tästä on seurannut se, että tietosuoja-asetuksen perustellusti henkilötietojen käsittelyyn liittyvät tiukat reunaehdot tulevat rekisterinpitäjien huomioitavaksi myös silloin, kun mahdollisuus yksittäisen rekisteröidyn tunnistamiseen on lähinnä spekulatiivista tai joka tapauksessa hyvin epätodennäköistä. Tämä hidastaa osaltaan julkishallinnon digitaalisten palvelujen kehittämistä.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Tietosuoja-asetuksen henkilötietojen käsittelyä koskevat periaatteet suojaavat hyvin ja tarkoituksensa mukaisesti luonnollisten henkilöiden henkilötietoja. Kuitenkin esimerkiksi 5 (1) artiklan b-alakohdan mukainen käyttötarkoitussidonnaisuuden periaate on koettu joissakin tapauksissa haastavaksi julkishallinnon kehityksen kannalta. Julkishallinnon organisaatioissa henkilötietoja käsitellään suurimmaksi osaksi lakisääteisten tehtävien hoitamista varten. Näitä tarkoituksia varten kerättyjä henkilötietoja olisi tarpeellista rajatuissa määrin käsitellä esimerkiksi uusien tietojärjestelmien loppuvaiheen testauksissa, mutta tämä merkitsisi lähtökohtaista poikkeusta asetuksen käyttötarkoitussidonnaisuuden vaatimukseen. Asetus mahdollistaa muun kuin alkuperäisen käyttötarkoituksen mukaisen käsittelyn silloin, jos se on yhteensopivaa alkuperäisen tarkoituksen kanssa. Yhteensopivan käsittelyn määritelmä ei kuitenkaan ole täsmällinen ja eri rekisterinpitäjät tulkitsevat sitä keskenään hyvinkin eri tavoin, mikä hankaloittaa julkishallinnon digikehityksen edistämistä kokonaisuutena. Olisikin hyödyllistä, mikäli tätä määrittelyä täsmennettäisiin asetuksen tasolla. Julkisen hallinnon palveluiden kehittämisen kannalta olisi myös hyödyllistä, mikäli asetus mahdollistaisi nykyistä selkeämmin henkilötietojen rajatun käsittelyn tällaisessa tietojärjestelmien kehitystarkoituksessa.

Tietosuoja-asetuksen 6 artiklan mukaiset henkilötietojen käsittelyperusteet ovat pääasiassa melko selkeitä ja vakiintuneita. Julkishallinnossa on kuitenkin toisinaan tilanteita, joissa olisi tarve eri käsittelyperusteiden laajemmalle hyödyntämiselle. Esimerkiksi rekisteröidyn suostumusta ei voida viranomaistoiminnassa pääsääntöisesti käyttää henkilötietojen käsittelyn perusteena, sillä tietosuoja-asetuksen johdanto-osan 43 kohtaan on kirjattu, että erityisesti viranomaisen ollessa rekisterinpitäjänä, on epätodennäköistä, että suostumus on annettu vapaaehtoisesti kaikissa kyseiseen tilanteeseen liittyvissä olosuhteissa. Digitaalisten palvelujen kehittämisessä ja laajemminkin viranomaisten palvelujen kehittämisessä olisi kuitenkin hyödyllistä, mikäli myös suostumusta voitaisiin hyödyntää käsittelyperusteena, esimerkiksi tietojärjestelmän testaamisessa. Tällöin rekisteröidyt voisivat myös itse vaikuttaa siihen, käsitelläänkö heidän henkilötietojaan palvelujen kehittämistarkoituksessa.

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

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

Vaikka säädöstasolla ero asetuksen 26 artiklassa tarkoitetun yhteisrekisterinpidon ja 28 artiklassa tarkoitetun henkilötietojen käsittelyn välillä vaikuttaa periaatteessa selvältä, ei asia käytännön rekisterinpitotilanteissa useinkaan ole näin yksiselitteinen. Monesti rajanveto sen välillä, onko kyse kahden tai useamman toimijan kesken järjestetystä yhteisrekisterinpidosta vai kuitenkin jonkun toimijan osalta pelkästään henkilötietojen käsittelystä, on häilyvä. Esimerkiksi erilaisten tietojärjestelmäratkaisujen hankinta- ja toteutusketjut voivat olla monessa vaiheessa tapahtuvia ja järjestelmien ylläpitoon osallistua usealla eri tasolla ja keskenään erilaisissa rooleissa olevia toisiinsa nähden itsenäisiä toimijoita. Tietojärjestelmien toiminnallista määrittelyä ja tuotannon ylläpitoa voi tapahtua useammassa eri ketjun vaiheessa ja useamman itsenäisen toimijan toimesta. Tällöin ei ole aina selvää, missä pisteessä jonkin toimijan rooli muodostuu niin merkittäväksi, että sen voidaan katsoa osallistuneen käsittelyn tarkoituksen ja keinojen määrittelyyn siten kuin asetuksen 26 artiklassa on säädetty. Tämän seurauksena myös ratkaisut tietyn toimijan roolista rekisterinpitäjänä tai henkilötietojen käsittelijänä vaikuttaisivat muodostuvan vaihteleviksi ja keskenään epäjohdonmukaisiksi eli kyse on tavallaan ns. ”veteen piirretystä viivasta” tässä asiassa. Toivottavaa olisikin, että tätä epätarkkarajaisuutta voitaisiin jatkossa vähentää ja pystyttäisiin laatimaan nykyistä paremmin ohjaavia kriteereitä sen ratkaisemiseksi, missä pisteessä henkilötietojen käsittely tosiasiallisesti muuttuu yhteisrekisterinpidoksi jonkin toisen toimijan kanssa.

Asetuksen 33 artikla edellyttää ilmoitettavaksi valvontaviranomaiselle kaikki sellaiset tietoturvaloukkaukset, joista voi aiheutua luonnollisen henkilön oikeuksiin tai vapauksiin kohdistuva riski. Ilmoitus on aina tehtävä 72 tunnin kuluessa loukkauksen ilmitulosta siitä riippumatta, minkä tasoinen riski loukkauksesta rekisteröidyn oikeuksille tai vapauksille tosiasiallisesti aiheutuu. Käytännössä merkittävä osa tietoturvaloukkauksista on varsin lieviä ja niistä rekisteröidyn oikeuksille tai vapauksille aiheutuva riski lähinnä teoreettinen tai joka tapauksessa hyvin vähäinen. Kuitenkin myös tällaisista loukkauksista on tehtävä ilmoitus saman 72 tunnin määräajan kuluessa, joka käytännössä on huomattavan lyhyt määräaika etenkin silloin, jos määräaikaan sisältyy viikonloppu tai juhlapyhiä. Lyhyehkö määräaika johtaa usein myös siihen, että ilmoitus joudutaan ensi vaiheessa tekemään huomattavankin vajavaisena ja myöhemmin antamaan asiassa toinen täydentävä

ilmoitus, kun tapahtuneeseen liittyviä yksityiskohtia on saatu selvitettyä ensivaiheen havaintoja perusteellisemmin.

Käytännössä 72 tunnin määräaika pakottaa organisaation käyttämään resursseja tapahtuman yksityiskohtien selvittämiseen ja dokumentointiin hyvin nopealla aikataululla silloinkin, kun jo valmiiksi on selvää, että loukkauksesta rekisteröidylle aiheutuva riski on tosiasiallisesti hyvin vähäinen. Tällainen useimmiten yllätyksellisesti tapahtuva resurssien nopea allokointi asetuksesta seuraavan ilmoitusvelvollisuuden täyttämiseksi ei organisaation itsensä näkökulmasta ole kaikissa tilanteissa tarkoituksenmukaista eikä se välttämättä mainittavasti edistä myöskään rekisteröidyn oikeuksien toteutumista, jos tapauksesta sen vähäisen luonteen vuoksi ei edellytetä informoitavaksi rekisteröityä itseään. Riskitasoltaan vähäisten tietosuojaloukkausten osalta tulisikin arvioida, voisiko niistä valvontaviranomaiselle tehtävän ilmoituksen määräaikaa pidentää nykyisestä 72 tunnista tai vaihtoehtoisesti ilmoituksen sisältövaatimuksia keventää suhteessa merkitykseltään vakavampiin tietosuojaloukkauksiin.

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

Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille on koettu julkishallinnon digikehityksen kannalta hyvin haasteellisiksi. Erityisesti tietosuoja-asetuksen V luvun henkilötietojen siirtoja koskevat säännökset ovat hidastaneet julkishallinnolle lähitulevaisuudessa välttämätöntä laajan mittakaavan pilvisiirtymää. Asetuksen V luvussa mainitut henkilötietojen siirtoperusteet ovat riittämättömiä erityisesti huomioiden se, että globaalien pilvipalvelujen yhtenä hyötynä on paikallisesti tuotettuja palvelumekanismeja parempi tietoturvallisuus. Heinäkuussa 2023 Euroopan komission antama Yhdysvaltoja koskeva vastaavuuspäätös edistää julkishallinnon pilvisiirtymää, mutta ei kuitenkaan anna tiedonsiirroille täysin vakaata pitkän aikavälin pohjaa. Näin ollen tietosuoja-asetuksen siirtovälineitä olisikin syytä tarkastella uudelleen ja laajentaa.

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

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

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

Hallinto- ja kehitysjohtaja, ylijohtaja Anu Nousiainen

Tietojohtaja Vesa Lipponen

VN/23930/2023-VM-4

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Lipponen Vesa 91296177Y	Nousiainen Anu 91306994W
2023-09-06	2023-09-06