

Asia: VN/19902/2021

Lausuntopyyntö rikosasioiden tietosuojalain toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Direktiivin täytäntöönpano

1. Rikosasioiden tietosuojalaki mahdollistaa sen, että rikosasioiden tietosuojalain sijasta tai sen lisäksi sovelletaan joiltakin osin erityislainsäädäntöä. Rikosasioiden tietosuojalakia on myös täydennetty usealla erityislailla. Puuttuuko rikosasioiden tietosuojalaista joiltakin osin tietosuojaa koskevia vaatimuksia, jotka olisi syytä huomioida yleislaissa?

Rikosasioiden tietosuojalain 62 §:ssä säädettyä vaitiolovelvollisuutta koskeva kohta tulisi arvioida tarkemmin. Nyt voimassa olevassa laissa vaitiolovelvollisuutta koskeva kohta viittaa viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 23 §:än, joka koskee vain salassa pidettäviä tietoja. Yleisesti tietosuojasäännöksissä rikostuomioita ja rikkomuksia koskevat tiedot ovat katsottu sellaisiksi, jotka muutoin ovat korotetun suojausveloitteen piirissä rekisteröidylle aiheutuvan riskin vuoksi. Tällaisia tietoja ei kuitenkaan aina salassapitosäännökset suojaa, vaan rikosasioiden tietosuojalaissa tarkoitettulla viranomaisilla on myös paljon sellaista aineistoa, joka on julkista, mutta joka rekisteröidyn näkökulmasta edellyttäisi korotettua suojaa, muun muassa vaitiolovelvoitteen kautta. Syytä on myös havaita, että rikosoikeudellisessa prosessissa eri viranomaisten käsitellessä samoja tietoja, saman tiedon osalta voi vaihdella se, onko tieto salassa pidettävää vai ei. Rekisteröidyn näkökulmasta henkilötiedon käsittelyyn liittyvä riski ja riskin mahdollisesta toteutumisesta aiheutuva haittavaikutus voi kuitenkin olla yhtä vakava, riippumatta viranomaiskäsittelyyn liittyvästä suojan tasosta. Todettakoon, että käsittelyn käsitteeseen (rikosasioiden tietosuojadirektiivi 3.) katsotaan kuuluvaksi myös sellainen henkilötietojen käsittely, jossa viranomainen luovuttaa esimerkiksi asiakirjoihin sisältyviä henkilötietoja ”asettamalla ne muutoin saataville”.

2. Onko hallinnonalalla voimassa tai suunnitteilla rikosasioiden tietosuojalain 13 §:stä poikkeavaa sääntelyä, mukaan lukien automatisoitu profilointi, jolla on merkittäviä vaikutuksia rekisteröityyn, sekä erityisiä henkilötietoryhmiä hyödyntävä profilointi kuten kasvontunnistus?

Oikeusministeriö vastaa tuomioistuinsektorin ja oikeushallinnon osalta lainsäädännön laatimisesta. Oikeusministeriö valmistelee automaattista päätöksentekoa koskevaa hallinnon yleislainsäädäntöä, mutta sen merkityksestä tuomioistuinsektorin näkökulmasta, ei vielä ole tässä vaiheessa tietoa, etenäkään niiltä osin, kun puhutaan rikosasian käsittelyyn liittyvästä toiminnasta. Tuomioistuinvirastossa on meneillään selvitys haastemiesten hakurobottiin liittyen, jolla pyritään

tehostamaan haastehakemusten toimittamiseen liittyvien yhteystietojen käsittelyä. Myös tuomioistuinten ratkaisujen julkaisemiseen ja pseudonymisointiin liittyen oikeusministeriössä on ollut käynnissä ANOPPI-hanke. Tulevaisuudessa Tuomioistuinvirasto tulee selvittämään tuomioistuinsektorilla automatisoitujen henkilötietojen käsittelyn käyttömahdollisuuksia esimerkiksi päätöksenteon tukena.

3. Onko hallinnonalalla suunnitteilla uusia erityislainsäädäntöhankkeita, joilla on tarkoitus panna täytäntöön joiltakin osin direktiivin säännöksiä?

Tiedossamme ei ole tällaisia hankkeita, mutta lainsäädäntöä olisi syytä täsmentää ja täydentää julkisuusperiaatteen sekä tietosuojan näkökulmasta.

Vaikka julkisuusperiaate ei suoranaisesti kuulu rikosasioiden tietosuojadirektiivin soveltamisalaan (rikosasioiden tietosuojadirektiivi 16 art.), joudutaan sen käytännön toteuttamisessa lähes poikkeuksetta arvioimaan tietosuojaan liittyviä kysymyksiä. Tuomioistuinten julkisuuteen ja henkilötietojen käsittelyyn (ml. tietojen luovuttamiseen ja tietopyyntöjen toteuttamiseen) liittyvä lainsäädäntö on sirpaloitunut lukuisiin eri lakeihin (muun muassa tietosuoja-asetus (679/2016), tietosuojalaki (1050/2018), laki henkilötietojen käsittelystä rikosasioissa sekä kansallisen turvallisuuden yhteydessä (679/2016), laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa (370/2007), laki oikeudenkäynnin julkisuudesta hallintotuomioistuimissa (381/2007), laki viranomaistoiminnan julkisuudesta (621/1999)).

Oikeudenkäynnin julkisuus on turvattu perustuslaissa ja kansainvälisissä ihmisoikeussopimuksissa. Julkisuudella suojataan asianosaista viranomaisen mielivaltaista toimintaa ja vapauden riistoa vastaan, varmistetaan oikeudenmukaista oikeudenkäyntiä sekä välitetään tietoa oikeusjärjestyksen sisällöstä, jotta ratkaisutoiminta on ennakoitavaa ja ennalta ehkäisevää. Edellä esitetyistä syistä johtuen, julkisuusperiaatteella on tuomioistuinten toiminnassa tavanomaisesta viranomaistoiminnasta poikkeava merkitys.

Samanaikaisesti on tunnistettava, että henkilötietojen suojalla on merkittävä rooli esimerkiksi oikeudenmukaisen oikeudenkäynnin toteuttamisen kannalta esimerkiksi sitä kautta, että asianosaiset uskaltavat kääntyä tuomioistuimen puoleen, esittää oikeudenkäynnissä vapaasti ja sensuroimatta oman näkemyksensä tapahtuman kulusta ilman pelkoa siitä, että oikeudenkäyntimateriaalia, esimerkiksi siitä kertyneitä nauhoitteita saatetaan internettiin saataville laajemmalle yleisölle, kuten tuoreessa Helsingin hovioikeuden käsittelemässä asiassa HO 2021:5 (Dnro R 20/2285) oli käynyt. Tietosuojalla on siis selkeä liitännä myös rikosasioiden tietosuojadirektiivin alaiseen rikosasian käsittelyyn tuomioistuimessa ja sitä kautta vaikutus esimerkiksi päätöksenteossa käytettävän tiedon laatuun. Asianomistajan yksityiselämän suojan toteutuminen rikosprosessissa ja erityisesti oikeudenkäynnin yhteydessä on nostettu tiedeyhteisössä tarkastelun kohteeksi ja vaatimuksia lainsäädännön uudistamisesta on esitetty myös tässä yhteydessä (kts. Satu Rantaeskolan väitöskirja). Joskus yksityisyyden suojan toteuttaminen jää oikeudenkäynnissä asianosaisten oman ymmärryksen, osaamisen ja vaatimusten varaan (kts. YTJulkL 10 §).

Tämän vuoksi, olisi erityisen tärkeää on tarkastella tätä kokonaisuutta ja kontekstia laajemmin myös tietosuojanäkökulmasta, rekisteröidyn sekä oikeuksien ja vapauksien näkökulmasta, tunnistuen rekisteröidyn heikompi asema ja siten, että rekisteröidyn henkilötietojen suojan toteutuminen tyhjene ainoastaan asiakirjan julkisuutta ja salassapitoa koskevaan tarkasteluun.

Tietosuojasäännöksiä näkökulmasta useat rikosasian yhteydessä käsiteltävät henkilötiedot kuuluvat korotetun suojausvaatimuksen piiriin, mutta siitä huolimatta tiedot voivat olla julkisia. Tämän vuoksi on huomattavasti yksityiskohtaisemmin arvioitava sitä, kuinka oikeudenkäynnin julkisuutta ja tietosuojaa koskevat vaatimukset sovitetaan käytännössä yhteen.

Oikeusministeriön tulisi mitä pikimmiten aloittaa myös tuomioistuinten toiminnan julkisuutta koskevan lainsäädännön tarkastelu nyt voimassa olevaa tietosuojalainsäädäntökehikkoa vasten, huomioiden myös rikosasioiden käsittelyyn liittyvät, usein korkeat riskit, eri asemassa olevien rekisteröityjen oikeuksien ja vapauksien kannalta. Tuomioistuinvirasto on nostanut tähän asiaan liittyviä haasteita esille osin jo lausunnossaan, joka koski viranomaisten ja julkisten tehtäviä hoitavien kokemuksia julkisuuslain toimivuuteen ja julkisuuslain periaatteeseen liittyen (VN 27452/2020).

Tuomioistuinsektorilla henkilötietojen käsittelyyn liittyvissä kysymyksissä kokonaiskuvan hallinta sekä lainmukaisen ratkaisun löytäminen yksittäisissä tapauksissa edellyttää lukuisten eri lakien ja säännösten yhtäaikaista soveltamista sekä syvällistä asiantuntemusta säännösten sisällöstä. Lainsäädännön sirpaleisuus, vaikeaselkoisuus sekä se, että eräiltä osin nyt voimassa olevan kansallisen sääntelyn soveltuvuutta on arvioitava EU-oikeuden etusijaisuusperiaatetta vasten, voivat osaltaan johtaa epäyhtenäisiin käytäntöihin esimerkiksi asiakirjojen julkisuutta koskevissa ratkaisuissa sekä osaltaan aiheuttaa riskin rekisteröityjen oikeuksille ja vapauksille. Tietosuojalainsäädäntökehikon muutos asettaa myös kovan paineen arvioida, ja tarvittaessa ajantasaistaa, oikeudenkäynnin julkisuutta koskevissa laeissa tehtyjä ratkaisuja. Vain tätä kautta voidaan todeta, että kansallinen lainsäädäntömme on arvioitu uudistunutta tietosuojasääntelyä vasten sen edellyttämällä tavalla.

Kun lainsäädäntöä tarkemmin arvioidaan tässä kontekstissa, on myös huomioitava ne tilanteet, joissa saman vastaajan useampia asioita kumuloidaan rikosasiassa yhteydessä yhdeksi kokonaisuudeksi ja se, kuinka tietosuoja tässä kontekstissa esimerkiksi eri asianomistajien kesken toteutetaan, kun oikeudenkäynti ja siitä syntyvä aineisto muodostaa käytännössä yhden kokonaisuuden (kts. tarkemmin rikosasioiden oikeudenkäyntilain ROL 5 luvun 18 §:esim. kutsu oikeudenkäyntiin tai tuomio, jossa asiaan liittyvät tiedot ovat yhdessä kokonaisuudessa). Kumulaatioharkintaan vaikuttaa olennaisesti rikoslain 6 ja 7 luvun säännökset rangaistuksen mittaamisesta ja yhteisestä rangaistuksesta. Kun tuomioistuinten toimintaa koskevaa lainsäädäntöä tarkistetaan tietosuojakehikkoa vasten, on myös samalla huomioitava tuomioistuimen käytännön työhön liittyvät vaatimukset.

On myös tarkemmin tarpeen tarkastella sitä, miten vastaajan rikosrekisteritietoja käsitellään. Rikosrekisterin tiedot on tarkoitettu pääasiallisesti viranomaiskäyttöön. Osa tuomioistuimista on sähköistänyt lähes koko asiakirjakäsittelynsä, mikä on osaltaan lisännyt käytäntöä lähettää

rikosrekisterin salattuna sähköpostina puolustajalle etukäteen tutustuttavaksi. Osa lähettää myös laatimansa ns. konkurrenssikaavion, jotta vastaajan näkemys yhteisen rangaistuksen mittaamisessa on helpompi muodostaa. Osa tuomareista taas käsittelee rikosrekisteritietoja suullisesti pääkäsittelyssä lukemalla rikosrekisterin tiedot. Vanhastaan käytäntö on ollut se, että paperille tulostettua rikosrekisterin otetta on näytetty puolustukselle, mutta kopioita siitä ei ole annettu asianosaisille. Toimintatapaa olisi syytä arvioida rikosasioiden tietosuojalain näkökulmasta.

4. Onko rikosasioiden tietosuojadirektiivissä säännöksiä, joiden täytäntöönpano erityislainsäädännössä on osoittautunut hankalaksi tai joiden merkitys on epäselvä?

Tietosuojadirektiivin 45 art. 2 kohdassa säädetään siitä, että ”Kunkin jäsenvaltion on säädettävä siitä, että valvontaviranomaisella ei ole toimivaltaa valvoa sellaisia käsittelytoimia, joita tuomioistuimet suorittavat lainkäyttötehtäviensä yhteydessä.” Edellä ehdotettu säännös on erittäin tulkinnanvarainen ja on osaltaan aiheuttanut myös sen, että toimintatavat ja tulkinnat ovat eri jäsenmaissa ratkaistu hyvin eri tavoin (Kts. Raportti ”Data protection in the judiciary: the concept of courts/judicial authorities acting in their judicial capacities, Final report, EDPS/2019/02-01). Tietosuojalainsäädännön osalta harmonisointi, erityisesti tuomioistuin lainkäyttötehtävien osalta, ei ole onnistunut tässä yhteydessä tulkinnanvaraisen tietosuojalainsäädännön johdosta.

Avaamme yksityiskohtaisemmin niitä kohtia, jotka jättävät edellä esitetystä säännöksessä tulkinnan varaa: Ensinnäkin epäselväksi jää se, mitä lainkäyttötehtävillä tarkalleen ottaen tarkoitetaan. Esimerkiksi, kun kehitetään tietojärjestelmiä, joita on tarkoitus käyttää nimenomaan lainkäyttötehtävien yhteydessä tai tuomioistuinten toimitilaturvallisuuteen liittyvissä yhteyksissä, voi herätä kysymys siitä, onko kysymys lainkäyttötehtäviin liittyvästä käsittelystä. Tietojärjestelmän ratkaisulla on suora vaikutus lainkäyttötehtävien yhteydessä tapahtuvaan käsittelyyn.

Rikosasioiden tietosuojadirektiiviin johdanto-osan kohdassa 80 todetaan, että ”Tämä poikkeus olisi rajattava koskemaan tuomioistuinten lainkäyttötehtäviä oikeudenkäynneissä, eikä sitä pitäisi soveltaa muuhun toimintaan, johon tuomarit saattavat osallistua jäsenvaltion lainsäädännön mukaisesti.” Kun edellä esitetyn lisäksi huomioidaan rikosasioiden tietosuojalain lainvalmistelussa laadittu materiaali (mm. lakivaliokunnan lausunto), ei se vielä sellaisenaan täsmennä tarpeeksi, mitä lainkäyttötehtäviin kuuluvaksi käsittelyksi voidaan katsoa. Tätä rajanvetoa tulisi selkeyttää lainsäädännön tasolla tai vähintäänkin valvontaviranomaisten toimesta.

Toiseksi, toimivaltarajaus koskee nimenomaan valvontaviranomaisen ”valvontaa”. Epäselvää on se, mitkä valvontaviranomaisen tehtävät katsotaan nimenomaan ”valvonnaksi” ja mitkä tehtävät ei. Esimerkiksi vaikutustenarvioinnin pohjalta tehtävän ennakokokuulemisen osalta (rikosasioiden tietosuojadirektiivi 28 art.) valvontaviranomaisen toimivalta on direktiivin 46 (46 art. 1 k-kohta) ja 47 (47 art. 3 kohta) artikloissa sidottu ”neuvontaan”. On tärkeää, että se, mitä nimenomaisesti katsotaan valvonnaksi selkeytetään myös sen vuoksi, että myös tuomioistuimilla olisi tiedossa, missä asiassa ne voivat kääntyä direktiivissä tarkoitettun valvontaviranomaisen puoleen sille määrättyissä tehtävissä. Käytännössä rajauksen epämääräisyys heijastuu erityisesti tietoturvaloukkauksien ilmoittamiseen liittyvään prosessiin, jossa epäselväksi jää kokonaisuudessaan se, onko

tuomioistuimen tehtävä ilmoitus valvontaviranomaiselle ja jos on, niin mille valvontaviranomaiselle? Valvontaviranomaisen toiminta osana tätä prosessia kirkastaa osaltaan sitä, miten rekisteröityyn kohdistuvia riskejä tulisi eri tietoturvaloukkaustilanteissa arvioida. Mikäli valvontaviranomainen ei ole osana tätä prosessia, jää myös rekisteröidylle ilmoittamisen kynnys puhtaasti tuomioistuinten oman arvioinnin varaan. Ottaen huomioon tuomioistuinten toimiala ja henkilötietojen käsittelyyn liittyvät riskit rekisteröityjen erityisesti rikosasioiden käsittelyn yhteydessä, olisi tätä ilmoitusvelvoitetta syytä selkeyttää. Syytä on myös todeta, ettei ilmoitusvelvollisuuden osalta ole säädetty poikkeusta tuomioistuimen lainkäyttötehtävien osalta (vrt. esimerkiksi nimenomainen poikkeus tietosuojavastaavan tehtävien osalta), vaan epäselvyys syntyy nimenomaan lainkäyttötehtäviä koskevasta valvontaviranomaisen toimivallan rajauksesta ja siitä, ettei selkeästi ole säädetty, mikä viranomainen tehtävää hoitaa tietosuojavaltuutetun sijasta niissä tilanteissa, kun kysymys on rikosasian käsittelystä ja lainkäyttötehtävistä tuomioistuimessa.

Kolmanneksi, tulisi selkeyttää sitä, koskeeko tehty rajausta vain ja ainoastaan tuomioistuimen toteuttamia käsittelytoimia. Mikä on edellä esitetyn rajauksen vaikutus esimerkiksi tilanteissa, joissa rikosasian lainkäyttötehtävään linkittyvä henkilötietojen käsittely on ulkoistettu esimerkiksi yksityisen sektorin toimijalle tai toisella valtion hallinnon toimijalle, kuten oikeusrekisterikeskukselle tai Valtorille. Eräs esimerkki henkilötietojen käsittelyn ulkoistamisesta on esimerkiksi tuomioistuintoimintaan lainkäyttötehtäviin liittyvien asiakirjojen kääntäminen. Myös toimitilaturvallisuuteen liittyvissä yhteyksissä henkilötietojen käsittelytoimintaa voidaan ulkoistaa. Oikeusrekisterikeskus ja Valtori puolestaan liittyvät erottamattomasti kaikkiin, myös lainkäyttötoiminnassa käytettäviin digitaalisiin työkaluihin.

Toinen selvyttä vaativa kokonaisuus on se, ulottuuko rikosasioiden tietosuojadirektiivin soveltamisala hallinto- ja erityistuomioistuinten toimintaan? Tätä on jouduttu pohtimaan käytännössä esimerkiksi tietojärjestelmää koskevissa kehittämishankkeissa. Hallinto- ja erityistuomioistuimissa ei käsitellä kansallisessa rikoslaissa tarkoitettuja rikoksia koskevia asioita. Hallinto- ja erityistuomioistuimissa kuitenkin käsitellään hallinnollisia sanktioita eli rangaistusluontoisia hallinnollisia seuraamuksia koskevia asioita (esimerkiksi erilaiset seuraamus-, rikkomus- ja laiminlyöntimaksut). Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään pitänyt monia erilaisia hallinnollisia sanktioita ihmisoikeussopimuksen 6 artiklan (oikeudenmukainen oikeudenkäynti) tarkoittamassa mielessä rikosoikeudellisina. Ihmisoikeussopimuksen 6 artiklalla ja sitä tulkinneella ihmisoikeustuomioistuimen oikeuskäytännöllä on keskeinen merkitys arvioitaessa myös unionin oikeudessa, erityisesti EU:n perusoikeuskirjan 47 artiklassa taatun oikeudenmukaisen oikeudenkäynnin edellyttämän suojan aineellista sisältöä. Kun otetaan myös huomioon rikosasioiden tietosuojadirektiivin johdanto-osan 13 kappaleessa todettu viittaus Euroopan unionin tuomioistuimen tulkintaan, on vähintäänkin mahdollista, että luonteeltaan rikosoikeudellisia hallinnollisia sanktioita olisi pidettävä myös rikosasioiden tietosuojadirektiivin tarkoittamassa mielessä rikosoikeudellisina. Tätä taustaa vasten olisi siis syytä täsmentää tarkemmin myös rikosasioiden tietosuojadirektiivin soveltamisalaa suhteessa hallintotuomioistuihin.

Henkilötietojen siirto kolmansiin maihin ja kansainvälisille järjestöille

5. Mitä sopimuksia, säännöksiä ja standardeja sovelletaan tietosuojan riittävyyden arviointiin, kun henkilötietoja siirretään kolmansiin maihin ja kansainvälisille järjestöille (ks. rikosasioiden tietosuojalain 41-42 §)?

-

6. Kokemuksenne henkilötietojen siirtoihin sovellettavista poikkeuksista (rikosasioiden tietosuojalain 43 §), jotka koskevat tietosuojan riittävyyttä?

-

7. Kokemuksenne rikosasioiden tietosuojalain 44 §:n (henkilötietojen siirto kolmansiin maihin yksityisille ja muille vastaanottajille) soveltamisesta?

-

8. Millä tavalla rikosasioiden tietosuojalain säännökset ovat vaikuttaneet toimivaltaisten viranomaisten väliseen tiedonvaihtoon kansallisesti, jäsenvaltioiden välillä ja Suomen ja kolmansien maiden välillä, huomioiden erityisesti rekisterinpitäjien väliseen luottamukseen liittyvät näkökohdat?

Monet EU-rikosoikeudelliset instrumentit perustuvat suoriin yhteyksiin, eli toimivaltainen viranomainen Suomessa ottaa suoraan yhteyttä toisen EU maan toimivaltaiseen viranomaiseen. Näissä yhteyksissä käsitellään usein myös henkilötietoja, koska ne ovat asian luonteen vuoksi välttämättömiä. Tuomioistuinviraston tiedossa ei ole tarkemmin, miten tässä kansainvälisessä kontekstissa ja tietojen vaihdossa on tarkemmin huomioitu tietosuojasäännöksistä tulevat vaatimukset.

Kansainväliseen yhteistyöhön liittyy myös seuraavanlainen haaste: tuomioistuin joutuu yhä useammin hankkimaan rikosrekisteritietoja ulkomailta ECRIS-järjestelmästä tai muun yhteistyön avulla. Toisissa valtioissa annettujen tuomioiden selvitys on virkavelvollisuus. Tätä on painotettu varsin tuoreessa prejudikaatissa KKO 2020:69. Ongelmia voi muodostua, jos Suomeen toimitetaan rikosrekisteriote, jossa on epäselvyyksiä. Mikä on menettelytapa ongelmien ratkaisemiseksi? Kysymyksellä on vaikutusta rikosasiassa tehtävässä päätöksenteossa sekä siinä käytettävien tietojen laadun näkökulmasta.

Kansainvälisessä kontekstissa on myös ilmennyt tilanteita, joissa kansallisen viranomaisen rekisteristä saadut tiedot ovat olleet epätäydellisiä sillä hetkellä, kun tietoja on käytetty päätöksenteossa tuomioistuimessa, koska jokin muu maa ei ole puitepäättöksen edellyttämällä tavalla toimittanut rekisteriin Suomen kansalaisen tuomioita. Tämä on voinut paljastua vasta vuosien jälkeen, kun lainvoimainen ratkaisu on tuomioistuimessa tehty. Myös tämä kysymys linkittyy tietojen laatuvaatimuksiin sekä toisaalta siihen, minkälaisia jatkotoimenpiteitä on enää tehtävissä tuomioistuimen toimesta, kun lainvoimaisella tuomioilla ratkaistua asiaa ei voi avata uudelleen. Asialla merkitystä muun muassa vastaajan oikeusturvan kannalta laajemminkin.

Kansainvälinen yhteistyö rikosasioissa on lisääntynyt viime vuosina paljon tuomioistuimissa. Tällä hetkellä esimerkiksi eurooppalaiset tutkintamääräykset lähetetään toiseen jäsenvaltioon sähköpostitse. Toiveena olisi saada käyttöön portaali, joka varmistaisi turvallisen sähköisen välittämisen rajojen yli. Euroopan komissiolla on käynnissä e-CODEX-hanke, mikä tarkoittaa teknisen

alustan luomista jäsenmaiden oikeusalan tiedonvaihtoon. Suomen toimenpiteitä käyttöönoton jouduttamiseksi olisi syytä tältä osin tehostaa, koska asialla on varmasti merkitystä myös tietosuojan kannalta.

Muut kokemukset rikosasioiden tietosuojalain soveltamisesta

9. Minkälaista rikosasioiden tietosuojalakia täydentävää ohjeistusta rekisterinpitäjä/tietosuojaviranomainen antanut henkilötietojen käsittelystä?

Rikosasioiden tietosuojadirektiivin osalta EDPB sekä tietosuojavaltuutetun laatima yleinen ohjausmateriaali on ollut suhteellisen niukkaa etenkin rekisterinpitäjien osalta. Nyt tässäkin lausunnossa nostettujen tietosuojasäännöksiin liittyvien haasteiden vuoksi olisi erityisen tärkeää, että valvontaviranomaisilta saataisiin kattavampaa ohjausmateriaalia rikosasioiden tietosuojadirektiivin ja -lain osalta. Rikosasioiden tietosuojalakia soveltavat viranomaiset ovat myös perustaneet yhteistyöverkoston, jossa pyritään myös yhdessä kehittämään osaamista sekä työkaluja rikosasioiden tietosuojatyöhön.

10. Millä tavalla henkilökunnan tietoisuutta rikosasioiden tietosuojalain vaatimuksista on pyritty parantamaan?

Tuomioistuinvirasto suunnittelee tuomioistuimessa rikosasioita käsitteleville sihteereille koulutusta rikosasioiden tietosuojalain osalta vuoden loppupuolella 2021. Saamamme palautteen mukaan tuomioistuinten henkilökuntaa ei ole juurikaan koulutettu erikseen rikosasioiden tietosuojalaista, vaan koulutus on painottunut enemmän yleiseen tietosuojakoulutukseen. Esiin tulevia ongelmia on ratkaistu noudattaen soveltuvien osin kansallista lainsäädäntöä. Tuomioistuinvirasto tulee tukemaan osaltaan tuomioistuinmies työtä rikosasioiden tietosuojalakiin liittyvän osaamisen kehittämisessä.

On huomattava myös se, että rikosasioiden tietosuojalaista tulevat vaatimukset liittyvät rikosasioiden käsittelyssä käytettäviin tietojärjestelmiin sekä niiden ominaisuuksiin sekä siihen, kuinka ne ohjaavat tietojärjestelmän loppukäyttäjää toimimaan. Tästä näkökulmasta katsottuna kyseisen lain vaatimukset on pyritty huomioimaan tietojärjestelmiä koskevassa kehitystyössä sekä käsittelyä koskevissa ohjeistuksissa.

11. Millä tavalla rekisteröidyn tarkastusoikeus (rikosasioiden tietosuojalain 23 ja 24 § sekä 29 §) on järjestetty? Miten paljon rekisterinpitäjä/tietosuojaviranomainen on vastaanottanut vuosittain (2019-2021) tarkastuspyyntöjä ja mitä tilanteita, rekistereitä tai tietoryhmiä ne ovat pääosin koskeneet?

Tuomioistuinvirastoon on oltu yhteydessä eri tuomioistuimista vain osassa rekisteröidyn tarkastusoikeutta koskevia asioita (arviolta noin 20 asiaa vuonna 2020, osa asioista on ollut sellaisia, joissa sama pyyntö on mennyt useaan tuomioistuimeen), joten kattavaa kuvaa tarkastuspyyntöjen osalta ei ole. Helsingin käräjäoikeudelta saadun tilaston mukaan rikosasioiden tietosuojalain mukaisia tarkastusoikeuteen liittyviä asioita on ollut seuraavasti: 2 kpl ajalla 8 – 12/2019, 7 kpl vuonna 2020 ja 5 kpl ajalla 1. – 26.8.2021.

Usein tarkastusoikeutta koskevat pyynnöt ovat olleet luonteeltaan tuomioistuinkohtaisia, joissa on pyydetty saada kaikki kyseisessä tuomioistuimessa olevat rekisteröityä koskevat tiedot. Näin tarkastusoikeutta koskeva pyyntö, ja sen toteuttamisen edellytykset ovat osin määräytyneet rikosasioiden tietosuojalain ja osin tietosuoja-asetuksen sekä sitä täydentävän tietosuojalain pohjalta. Rekisteröidyn henkilöllisyyden todentamista koskevat vaatimukset ovat osin erilaiset ja helposti käytettäviä vahvan tunnistamisen mahdollistavia työkaluja kaivattaisiin tarkastusoikeuden käytön tukemiseksi laajemminkin, erityisesti nyt pandemia aikaan, kun asiointi tuomioistuimiinkin on tapahtunut pitkälti puhelimen tai sähköpostin välityksellä.

Rikosasioiden tietosuojalakiin liittyvien tarkastusoikeuspyyntöjen osalta haasteellisiksi kysymyksiksi ovat osoittautuneet pyynnöt, joissa rekisteröity on pyytänyt saada tietää, kenelle kaikille häntä koskevia tietoja on luovutettu. Rikosasioiden tietosuojalain 23 §:n 1 mom. 4 kohdan mukaan rekisteröidyllä on oikeus saada tieto ”vastaanottajista tai vastaanottajaryhmistä, joille rekisteröidyn henkilötietoja on luovutettu”. Rikosasioiden tietosuojalain 3 §:n 8 kohdan mukaan vastaanottajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja. Myös rikosasioiden tietosuojalain 19 §:n mukaisista lokitiedoista on selvittävä mm. kyselyn ja luovutuksen peruste, toteutuspäivä- ja aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen sekä niitä luovuttaneen henkilön tiedot ja näiden vastaanottajien henkilöllisyys. Rikosasioiden tietosuojalain hallituksen esityksen perusteluissa todetaan, että myös puhelimitse tulevista tiedoista on kirjattava edellä mainittua lokitusta koskevan säännöksen mukaiset tiedot. Haaste linkittyy asiakirjapyyntöihin; tuomioistuimista pyydetään paljon rikostuomioita, niin yksittäisten kansalaisten kuin lukuisten eri tahojen toimesta. Edellä esitetyn säännösten mukaisesti jokaista rikostuomioita koskeva asiakirjapyyntö tulisi kirjata siten, että myös sen henkilön tiedot, joka tietoja on pyytänyt, jäävät tuomioistuimelle talteen rekisteröityä koskevan asian yhteyteen. Nämä tiedot olisi edelleen annettava rekisteröidylle tarkastusoikeutta koskevan pyynnön yhteydessä. Kun pohditaan tarkemmin tuomioistuinten toimialaa, etenkin rikosasioiden puolella, voi tällä asialla olla paljon merkitystä tietopyynnön esittäjän näkökulmasta. Ottaen huomioon, miten julkisuusperiaatteen toteuttamisesta on muuten säädetty, olisi tätä ajatusta syytä tarkastella myös kansallisen lainsäädännön tasolla tarkemmin. Todettava myös on, että aiemmin on katsottu, ettei tietojärjestelmiin kertyvät lokitiedot ole rekisteröityä koskevia tietoja ja niitä ei tarkastusoikeuden perusteella olisi luovutettava. Tietoja voidaan kuitenkin pyytää julkisuuslain mukaisen asianosaisjulkisuuden perusteella. Haasteena kuitenkin on, että rekisteröidyn tarkastusoikeus vaikuttaisi nyt voimassa olevin säännöksin jo ulottuvan osin samoihin tietoihin kuin lokitiedot eli niihin tahoihin, joille tietoja on luovutettu (nk. vastaanottajat). Vastaanottajatietojen, lokitietojen, tarkastusoikeuden sekä asiakirjajulkisuuden välistä suhdetta olisi syytä arvioida yksityiskohtaisemmin myös lainsäädännön tasolla. Tällaisia tarkastusoikeuteen liittyviä pyyntöjä on tullut useampia eri tuomioistuimiin.

12. Onko rikosasioiden tietosuojalain soveltamisalaan kuuluvan henkilötietojen käsittelyyn nimetty tietosuojavastaava ja/tai mikä on rikosasioiden tietosuojalain soveltamisalaan kuuluvan käsittelyn valvontaan osoitetun henkilökunnan lukumäärä?

Tuomioistuimien lainkäyttötehtäviin liittyvä henkilötietojen käsittely on rikosasioiden tietosuojalaissa kokonaisuudessaan rajattu tietosuojavastaavan tehtävien ulkopuolelle (40 §:n 2 mom.), mutta muilta osin tietosuojavastaavat on nimetty. Tuomioistuimet on myös säädetty tietosuojavaltuutetun valvontatoimivaltuuden ulkopuolelle (45 §:n 2 mom.). Rikosasioiden

tietosuojadirektiivin 80 resitaalissa todetaan: ”Joka tapauksessa sitä, että tuomioistuimet ja muut riippumattomat oikeusviranomaiset noudattavat tämän direktiivin sääntöjä, on aina valvottava riippumattomasti perusoikeuskirjan 8 artiklan 3 kohdan mukaisesti.”. Rikosasioiden tietosuojalakia koskevassa hallituksen esityksen (HE 31/2018) perusteluissa on todettu, että ”Perustuslain 108 ja 109 §:ssä säädetyn mukaisesti oikeuskansleri ja oikeusasiamies valvovat tuomioistuinten toiminnan lainmukaisuutta. Ne valvovat siten myös sitä, että tuomioistuimet noudattavat kaikessa toiminnassaan henkilötietojen suojaa koskevaa lainsäädäntöä.” Siitä, kuka tosiasiaa valvoo tuomioistuinten osalta henkilötietojen käsittelyn lainmukaisuutta kansallisesti perusoikeuskirjan 8 artiklan mukaisesti, ei ole kansallisesti säädetty lain tasolla ja vaikuttaa siltä, ettei tuomioistuinten osalta valvontaa ole vastuutettu selkeästi kenellekään. Tämä on aiheuttanut epäselvyyttä tietosuojasäännösten mukaisista menettelytavoista tuomioistuinsektorilla ja toiveen siitä, että asiaa selkeytettäisiin lainsäädännön tasolla. Kysymys nousee esille muun muassa tietoturvaloukkausten, ennakkokuulemisten sekä rekisteröityjen informointien ja rekisteröidyn oikeuksien käyttämisen (mm. tietosuojavaltuutetun välityksellä) yhteydessä. Vastuun selkeyttämisen lisäksi on arvioita valvontaviranomaisen resursseja sekä sille asetettuja tehtäviä niiden edellyttämiin toimivaltuuksiin ja rekisterinpitäjän velvoitteisiin.

Tuomioistuinten tulee osaltaan myös noudattaa täysimääräisesti tietosuojalainsäädäntöä. Tätä taustaa vasten kansallisessa sääntelyssä tehty raja, joka ei jätä tuomioistuimelle itselleen harkintavaltaa tietosuojatyön järjestämisen osalta ja rajaa kaikki tietosuojavastaavan tehtävät tuomioistuimen rikosasioiden käsittelyyn liittyvien lainkäyttötehtävien ulkopuolelle, olisi syytä arvioida uudelleen. Esimerkiksi akuutissa lainkäyttötehtävään liittyvässä tietoturvaloukkauksessa voi olla rekisterinpitäjän, sekä ennen kaikkea rekisteröidyn edun mukaista, että tietosuojaan liittyviä neuvoja olisi nopeasti saatavilla sellaiselta taholta, joka jokaiseen organisaatioon on jo nimitetty ja jolla osaamista ja kokemusta tietosuojaan liittyvistä työtehtävistä. Usein tämä henkilö on nimenomaan tietosuojavastaava. Nykyisessä lainsäädäntökehikossa on osin kyseenalaista, voidaanko tietosuojavastaavan puoleen kääntyä tai voiko tietosuojavastaava omalta osaltaan muutoin auttaa silloin, kun on kysymys rikosasioiden tietosuojasääntelyn alaan kuuluva asiasta tuomioistuimessa.

13. Onko rikosasioiden tietosuojalain noudattamisessa ilmennyt ongelmia ja mitä säännöksiä ongelmat ovat erityisesti koskeneet?

Ei ole selvää eikä tarkkarajaista, mikä katsotaan rikosasian käsittelemiseksi tuomioistuimessa ja minkä aikaa rikosasioiden tietosuojalakia sovelletaan tuomioistuimessa käsiteltävänä olevaan rikosasiaan? Missä vaiheessa asia siirtyy rikosasioiden tietosuojalain soveltamisalan ulkopuolelle ja tietosuoja-asetuksen soveltamisalan piiriin? Tässä on huomioitava koko asian elinkaari vireille tulosta sen arkistointiin, jolloin sen käsittelyyn voi olla yhä tarvetta esimerkiksi ratkaisun yhdenmukaisuuden turvaamiseksi.

Ongelmana on jossain määrin lain soveltamisala ja erityisesti sen suhde muihin lakeihin, kuten tietosuojalakiin, lakiin viranomaisten toiminnan julkisuudesta ja lakiin oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa. Kuten edellä on todettu, useat käytännön kysymykset edellyttävät usean lain yhtäaikaista soveltamista, jolloin oikein ratkaisun löytäminen voi olla haastavaa.

Rikosasioden tietosuojalain 2 §:n 4 kohtaa olisi syytä täsmentää sanamuodoltaan direktiiviä vastaavaksi. Nyt käytetty sanamuoto hämmentää osin soveltamisalaa sen osalta, milloin ”rekisterin” muodostumista on arvioitava: ”Tätä lakia sovelletaan kuitenkin vain sellaiseen 1 ja 2 momentissa tarkoitettuun henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista tai jossa käsiteltävät tiedot muodostavat tai niiden on tarkoitus muodostaa rekisteri tai sen osa.” Direktiivin 2 artiklan osalta tämä käy selkeämmin esille, kun rekisterin muodostuminen keskittyy ”..sellaisen henkilötietojen muuhun kuin automatisoituun käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa”. Olisi siis syytä selkeyttää sitä, ettei ns. automaattisen ja sähköisen aineiston osalta ole tarve pohtia rekisterin muodostumista.

Edellä kohdassa 12. on nostettu jo esille tuomioistuinten toimintaa liittyviä epäselvyyksiä siltä osin, kun valvontatehtävään liittyvästä toimivaltuudesta ei ole säädetty tarpeeksi tarkkarajaisesti. Tähän tuomioistuinsektori toivoo selkeytetystä.

Edellä kohdassa 11. on nostettu myös haaste siitä, minkälaisia kysymyksiä rekisteröidyn tarkastusoikeuden yhteydessä on noussut esille, kun pyynnön kautta halutaan selvittää sitä, kenelle kaikille rikostuomioita koskevia tietoja on luovutettu.

Tietosuojalaissa on tehty myös eräitä kansallisia ratkaisuja, joiden perusteita ei olla lainsäädäntötyön yhteydessä tarkemmin avattu, ja jotka tosiasiaissa aiheuttavat merkittävää hallinnollista taakkaa käytännön tietosuojatyöhön. Ensimmäinen näistä on vaikutustenarviointia koskevaan vaatimukseen tehty muutos, joka nykyisessä sanamuodossaan, erityisesti huomioiden henkilötietojen käsittelyn konteksti, on käytännössä tehtävä lähes kaikesta henkilötietojen käsittelystä. Rikosasioden tietosuojalaissa 20 §:n 2 mom. mukaan ”Rekisterinpitäjän on tehtävä kirjallinen vaikutustenarviointi, jos suunniteltu henkilötietojen käsittely saattaa aiheuttaa merkittävän riskin luonnollisen henkilön oikeuksien toteutumisen kannalta”. Rikosasioden tietosuojadirektiivissä 27 art. 1 kohdan mukaan vaikutustenarviointi on laadittava, ”Jos tietänyttyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin..”. Merkittävä riski aiheutuu henkilötietojen käsittelystä huomattavasti useammin kuin korkea riski. Vaikutustenarvioinnin osalta on havaittava, että riskin vakavuus on usein sidottu henkilötietojen käsittelytyyppiin sekä asiakontekstiin ja sitä ei usein saada laskettua, vaan suojatoimenpiteillä voidaan lähinnä vaikuttaa riskin todennäköisyyteen. Ottaen huomioon rikosasioden tietosuojalain käsittelykonteksti ja käsittelyn vaikutukset rekisteröidyn oikeuksiin ja vapauksiin, on erittäin vaikeaa keksiä sellaisia käsittelytoimia, joista rekisteröidylle ei saataisi aiheutua merkittävää riskiä. Epäselväksi on jäänyt myös se, miksi on nähty tarpeelliseksi kansallisesti näin olennaisesti poiketa direktiivin tekstistä sekä laskea kirjallisten vaikutustenarviointien osalta rimaa siten, että se koskee lähes kaikkia käsittelytoimia. Myöskään hallinnollisia tai taloudellisia seuraamuksia ei tämän muutoksen osalta ole tarkemmin arvioitu. Todettakoon, että myös tietosuojavaltuutetulle ilmoitusvelvollisuus on sidottu tähän merkittävään riskiin ja johtuen tietojen luonteesta sekä käsittelykontekstista, tulee käsittelyyn liittyvä riski usein pysymään merkittävällä tasolla suojatoimenpiteistä huolimatta.

Rikosasioiden tietosuojalain 36 §:ssä on tehty myös kansallinen myös laajennus, jolla on laajennettu henkilötietojen tietoturvaloukkauksen ilmoitusvelvoitetta Suomessa toimiville rekisterinpitäjille. Tässä on tehty kansallinen laajennus rikosasioiden tietosuojadirektiivin 30 art. 6 kohtaan ilman, että on tarkemmin tarkasteltu veloitteesta aiheutuvaa hallinnollista taakkaa. Rikosasioiden tietosuojadirektiivin 30 art. 6 kohta edellyttää ilmoittamista vain toisen jäsenvaltion rekisterinpitäjälle. Rikosasioiden tietosuojalain 36 §: mukaan ”Rekisterinpitäjän on ilman aiheutonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta sellaiselle Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle, jonka toimittamiin tai jolle toimitettuihin tietoihin loukkaus kohdistuu.” Säännöksessä ei ole asetettu mitään reunaehtoja sen osalta, että minkälainen riski (matala riski, riski, merkittävä riski, korkea riski) kyseiseen tietoturvaloukkaukseen liittyy, vaan ilmoitus tulisi tehdä kaikista loukkauksista. Säännös ei myöskään sisällä mitään tarkoituksenmukaisuusharkintaa sen osalta, onko ilmoittaminen esimerkiksi tietosuojanäkökulmasta arvioiden perusteltua vai ei, tai aikajanaa sen suhteen, milloin toimitetuista tiedoista on kysymys. Tätä taustaa vasten, tehtyä kansallista ratkaisua olisi syytä arvioida vielä uudelleen, erityisesti tarkoituksenmukaisuuden ja hallinnollisen taakan näkökulmasta. Kokemuksemme mukaan, pääosa tietoturvaloukkauksista on ns. matalan riskin loukkauksia, joista ei ole odotettavissa mitään käytännön seuraamuksia tai haittavaikutuksia rekisteröidylle.

Lopuksi kiinnitän vielä huomioita eri lakien välisten vaatimusten ristiriitaisuuteen; esimerkiksi viranomaisen asiakirjoihin ja tiedonhallintaan liittyvät vaatimukset edellyttävät asiakkaan toimittaman aineiston, joka voi sisältää hyvinkin arkaluonteisia tietoja, kirjaamista ja säilyttämistä. Toimitettu aineisto voi kuitenkin olla viranomaisen toiminnan ja toimivallan näkökulmasta tarpeetonta. Epäselväksi jää, kuinka viranomainen voi tässä kontekstissa toteuttaa esimerkiksi tietosuojasääntelyyn liittyvää tarpeellisuusvaatimusta tai rekisteröidyn oikeuksiin liittyvää vaatimusta tietojen poistamisesta, kun tietoa ei voida poistaa sen tarpeettomuudesta huolimatta rekisterinpitäjän lakisääteisistä veloitteista johtuen.

14. Näkemyksenne lainsäädännön toimivuudesta tietosuojaviranomaisen valvontavaltuuksien käytön ja laillisuusvalvonnan näkökulmasta?

Tuomioistuinten näkökulmasta arvioituna, nyt tehty kansallinen ratkaisu edellyttää selkeyttämistä tämän lausunnon kohdassa 12. esitettyjen perustelujen johdosta. Nykyinen tilanne ei täytä perustuslaissa edellytettyä täsmällisyyden ja tarkkarajaisuuden vaatimusta valvontavaltuuksien tai muun laillisuusvalvonnan osalta.

15. Onko rikosasioiden tietosuojalain 51 ja 52 §:n säännöksiä vielä sovellettu ja jos kyllä, minkälaisissa tilanteissa?

Tuomioistuinviraston tiedossa ei ole, että kyseisiä säännöksiä (51 § toimenpiteet, 52 § uhkasakko) olisi tuomioistuinsektorilla sovellettu. Myös tämän asian osalta merkityksellinen on valvontaviranomaisen tehtäviin ja toimivaltuuksiin liittyvien epäselvyyksien tuomioistuinten osalta.

16. Kokemuksenne rikosasioiden tietosuojalain säännösten ja rikosoikeudellisen ja virkamiesoikeudellisen sääntelyn yhteentoimivuudesta?

Tietosuoja säännöksiin liittyvät velvoitteet tulee rakentaa nimenomaan rekisterinpitäjän vastuuseen, johon kuuluu myös henkilötietojen käsittelyn osalta selkeiden ohjeiden, kattavan koulutuksen ja turvallisten työkalujen varmistaminen. Vastuuta henkilötietojen lainmukaisesta käsittelystä ei voi jättää yksittäisen virkamiehen tai muun toimijan oman osaamisen, valvutuneisuuden ja harkinnan varaan. Digitaalisessa toimintaympäristössä yksittäisen loppukäyttäjän voi olla hyvin vaikea, jollei mahdotonta arvioida henkilötietojen käsittelyyn liittyviä riskejä esimerkiksi silloin, kun viestin vaihtoa käydään erilaisilla sähköisillä alustoilla, riippumatta siitä, kuka viestintätyökalun tarjoaa. Virkamiehen on pystyttävä luottamaan siihen, että noudattamalla rekisterinpitäjän ohjeita henkilötietojen käsittelystä ja käyttämällä työnantajan tarjoamia työvälineitä, hän täyttää oman osansa tietosuojaan liittyvistä velvoitteista.

17. Mahdolliset huomionne henkilötietojen käsittelyn tietoturvallisuutta koskevista vaatimuksista (suunnitelmat, ohjeet, tietojärjestelmämuutokset, organisatoriset muutokset, auditoinnit, tietoturvaloukkauksia koskevat ilmoitukset), huomioiden myös lokitietojen osalta täytäntöönpanoon varattu siirtymäaika

Tuomioistuinsektorilla on siirrytty uusiin tietojärjestelmiin, joissa lokitusta koskevat vaatimukset on huomioitu. Vaikka järjestelmiä uusitaan, on huomattava, että vanhoissa järjestelmissä olevia tietoja saatetaan joutua hyödyntämään vielä pitkäänkin esimerkiksi ratkaisukäytännön yhdenmukaisuuden varmistamiseksi. Myös näiden järjestelmien osalta lokitusvaatimuksia on tarkasteltu ja päivitetty.

Viitaten jo kohdassa 4. esitettyyn epäselvyyteen rikosasioiden tietosuojalain soveltuvuudesta hallinto ja -erityistuomioistuinten toimintaan, on lisäksi todettava, ettei tuomioistuimeen tulevasta asiasta voida ennalta kategorisesti tehdä päätelmiä siitä, mitkä tapaukset kuuluvat rikosasioiden tietosuojalain soveltamisalaan, koska tämä on viime kädessä tuomioistuimen ratkaisuun ja siitä annettavaan seuraamukseen liittyvä asia. Koska tilanne kuitenkin on se, että jos asia saattaa kuulua rikosasioiden tietosuoja sääntelyn soveltamisalaan, on tästä laista seuraava, muun muassa joustamaton lokitusvaatimus, ulotettava koko järjestelmään. Tällä on vaikutuksia järjestelmän kokonaiskustannuksiin.

Tuomioistuinsektorilla, erityisesti ratkaisukäytännön yhdenmukaisuuteen liittyvät vaatimukset, vaikuttavat merkittävästi myös siihen, kuinka tiukkoja rajoituksia ja suojatoimenpiteitä voidaan käytettävissä tietojärjestelmissä henkilötietojen osalta tehdä. Tätä taustaa vasten myös kertyvän lokitiedon laajuus asettaa omat haasteensa erityisesti jälkikäteisen valvonnan osalta.

On myös huomattava, että joitakin henkilötietojen käsittelyyn liittyviä palveluja voidaan joutua hankkimaan eri tahoilta, esimerkiksi kääntämiseen liittyen. Näissä konteksteissa rikosasioiden tietosuojalakiin liittyvät vaatimukset, muun muassa lokitietojen osalta voivat luoda erityisen haasteen määrättyjen palvelujen käyttöönotolle, vaikka käsittelykonteksti muutoin olisi ns. matalariskinen.

18. Mahdolliset huomionne rikosasioiden tietosuojalain vaikutuksista uuden teknologian kehittämiseen ja käyttöön

Kun rikosasioiden tietosuojalaki asettaa yksityiskohtaisia vaatimuksia sille toimintaympäristölle, missä henkilötietoja voidaan ylipäättään käsitellä, on myös tunnistettava, että tällaisista vaatimuksista on merkittäviä heijastuksia palvelujen kustannuksiin ja/tai esimerkiksi siihen, millä aikataululla tiettyjä palveluja voidaan tuottaa. Nämä vaatimukset heijastuvat kaikkeen tulevaan digitalisaatioon ja henkilötietojen käsittelytoimiin myös tuomioistuinsektorilla ja tämä tulisi asianmukaisesti huomioida hankkeiden sekä tuomioistuinsektorin rahoituksessa. Tuomioistuimen keskeinen rooli oikeusturvan toteuttajana tulee ottaa huomioon toimintaedellytyksistä sekä määrärahoista päätettäessä.

Todettakoon myös, että oikeushallinnon tietojärjestelmien kehittämiseen vaikuttava monikerroksinen ja useiden eri viranomaisen luoma rakenne (Oikeusministeriö, Tuomioistuinvirasto, Oikeusrekisterikeskus, Valtori sekä tuomioistuin) ei osaltaan helpota tietosuojasääntelyyn liittyvän kokonaiskuvan luomista sekä säännösten edellyttämien vaatimusten tosiasiallisen toteutumisen arviointia. Myös tietosuojasäännöksistä kumpuavien roolien, vastuiden ja velvoitteiden hahmottaminen voi olla hyvinkin haastavaa tässä monitoimijakokonaisuudessa. Tässä kontekstissa tulisi arvioida tarkemmin myös esimerkiksi käsittelysopimuksiin liittyviä vaatimuksia sekä niiden hallintaa ja arvioida sitä, voitaisiinko näiltä osin tietosuojasääntelystä seuraavia vaatimuksia keventää tai yksinkertaistaa esimerkiksi lainsäädännöllisillä keinoilla? Myös yhteisrekisterinpitäjyyden mahdollistamaa vastuunjakoa tietosuojavelvoitteiden osalta tulisi tarkastella tarkemmin organisaatiota koskevan lainsäädännön yhteydessä muun muassa päällekkäisen työn ja tarpeettoman hallinnollisen taakan keventämisen näkökulmasta.

19. Muut mahdolliset huomionne rikosasioiden tietosuojadirektiivistä tai rikosasioiden tietosuojalaista ja sen soveltamisesta

Tuomioistuinvirasto on tässä lausunnossaan tuonut esille niitä käytännön kokemuksia ja haasteita, joita se on kohdannut rikosasioiden tietosuojadirektiiviä sekä rikosasioiden tietosuojalakia tulkitessaan. Tuomioistuinvirasto tiedotti nyt kysymyksessä olevasta lausuntopyynnöstä koko tuomioistuinsektoria ja osa tässä lausunnossa esitetyistä huomioista on tullut suoraan tuomioistuimilta Tuomioistuinvirastolle nostettavaksi esille tämän lausuntopyynnön yhteydessä.

Suuri haaste, johon hyvin pikaisesti toivotaan selkeytystä, on nimenomaan valvontaviranomaisen toimivalta suhteessa tuomioistuimiin sekä tästä epäselvyydestä seuraavat heijasteet päivittäiseen tietosuojatyöhön, kuten tietoturvaloukkausten ilmoitusmenettelyyn. Ottaen huomioon tuomioistuinsektorin henkilötietojen käsittelyyn liittyvät erityiset vaatimukset, oikeusministeriön voi olla syytä harkita, tarvitaanko henkilötietojen käsittelystä oma erityislakinsa, kuten monella muulla toimivaltaisella viranomaisella henkilötietojen käsittelyn osalta on.

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Jaakkola Riku
Tuomioistuinvirasto

Leivonen Raisa
Tuomioistuinvirasto