Tietosuojavaltuutetun toimisto

Dnro 3422/03/2017

15.12.2017'

Oikeusministeriö
lausuntopalvelu.fi

lausuntopyyntönne 7.11.2017 OM 21/41/2016

Lausunto ehdotuksesta henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä

Johdanto

Lakiehdotuksen tarkoituksena on panna täytäntöön EU:n direktiivi (2016/680, lyh. RtsD = rikosasioiden tietosuojadirektiivi) luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten. Näiden tarkoituksien edellyttämä henkilötietojen käsittely voidaan jakaa karkeasti ottaen kolmentyyppiseen henkilötietojen käsittelyyn.

Ensinnäkin kun puhutaan henkilötietojen käsittelystä rikosten ennalta estämisen tarkoituksessa, on kyse sellaisesta yksilöityä tekijää koskevasta tiedonhankinnasta, jonka perusteella voidaan tekijän toimintaan puuttua ennen rikoksen täyttymistä. Toisena käsittelytyyppinä voidaan pitää ns. käänteistä käsittelyä (reverse), jossa esitutkinta aloitetaan tekoja tai laiminlyöntejä taikka niiden seurauksia koskevista havainnoista ja ilmoituksista ja esitutkinnan keskeinen tarkoitus on saada yhdistettyä teko tekijään rikosvastuun toteuttamiseksi. Tällöin esitutkinnassa on kyse tällaisen henkilötiedollisen epävarmuuden selventämisestä ja ratkaisemisesta pitäen kuitenkin lähtökohtana sitä, että epäiltyä on pidettävä syyttömänä, kunnes hänen syyllisyytensä on laillisesti näytetty toteen (EU:n perusoikeuskirja 48 artikla). Tuomioistuimen tehtävänä on arvioida hankittua henkilöön viittaavaa tietoa tai näyttöä ja ratkaista se, onko epäillyn syyllisyydestä saatu riittävä näyttö. Kolmantena käsittelytyyppinä voidaan pitää lainvoimaisen syyllisyyden vahvistamisen jälkeistä käsittelyä rikosvastuun toteuttamiseksi kuten rangaistusten täytäntöön panemiksi ja sen jälkeistä käsittelyä muissa laillisissa käyttötarkoituksissa, kunnes tiedot ovat tulleet näissä tarkoituksissa tarpeettomiksi.

Pykäläkohtaiset kommentit
1 Luku Yleiset säännökset

1 § Soveltamisala

Kansallisena ratkaisuna on ehdotukseen sisällytetty 2 momentissa mainitut

Postiosoite	Käyntiosoite	Puhelin	Sähköposti	Kotisivut
PL 800	Ratapihankatu 9 Helsinki			
00521 Helsinki	6. krs	029 566 6700	tietosuoja@om.fi	http://www.tietosuoja.fi

Puolustusvoimien, poliisin ja Rajavartiolaitoksen tietyt lakisääteiset tehtävät. Poliisin ja Rajavartiolaitoksen osalta on kyse EU-oikeuden ulkopuolelle jäävästä lähinnä kansallisen turvallisuuden suojaamisen tarkoituksessa tapahtuvasta käsittelystä. EU:n tietosuojasääntely perustuu niin RtsD kuin EU:n yleinen tietosuoja-asetuksen (2016/579, lyh. TsA) osalta kuuteen tietosuojaperiaatteeseen, on mielestäni perusteltua ottaa sääntelyn perustaksi myös näiltä osin nämä tietosuojaperiaatteet.

Puolustusvoimien osalta soveltamisala näyttää ongelmalliselta, koska ehdotuksen mukaan se kattaisi kaikki puolustusvoimista annetun lain 2 §:n 1 momentin tehtävät erottelematta tarkemmin sitä, että jotkin puolustusvoimien tehtävät voivat kuulua soveltamisalaan jo 1 §:n 1 kohdan perusteella (esitutkinta) ja jotkin tehtävät voivat kuulua TsA:n alaan kuten pelastustoimintaan osallistuminen antamalla käytettäväksi pelastustoimintaan tarvittavaa kalustoa, henkilöstöä ja asiantuntijapalveluja ja jotkin tehtävät eivät kuulu EU-oikeuden soveltamisalaan.

2 § Suhde muuhun lainsäädäntöön

Rikosten ennalta estämisessä ja rikosoikeudellisessa prosessissa käsitellään henkilötietoja monissa yhteyksissä ja monin keinoin. Informaatio-oikeudellisesti sovellettavaksi voi tulla myös säännökset viranomaisten asiakirjoista ja niiden julkisuudesta ja salassa pidettävyydestä (julkisuuslaki) sekä pakkokeinoja todistusoikeudelliset tiedonhankintaa ja käsittelyä koskevat säännöt. Tästä syystä olisi tarpeen tarkemmin tarkastella ehdotuksen suhdetta näihin muihin informaatio-oikeudellisiin säännöksiin. Vaikka ehdotuksen 2 §:n 1 momentissa on todettu, että jos muussa laissa on ehdotetusta laista poikkeavia säännöksiä, ei tällainen toissijaisuussäännös vielä ratkaise tilanteita, joissa ei ole niinkään kyse poikkeavista säännöksistä vaan rinnakkaisesti ja jopa suojattavan oikeushyvän näkökulmasta jännitteisesti sovellettavista säännöksistä.

Ehdotuksen 2 §:n 2 momentti ei myöskään ratkaise normikollisioita, mitkä voivat johtua siitä, että EU:n tietosuojauudistuksen myötä sääntely yhä enemmän irtoaa henkilörekisteripohjaisesta sääntelystä kohti automatisoitua henkilötietojen käsittelyä, jota voidaan yhä laajemmin soveltaa myös asiakirjapohjaiseen (julkisuuslaki) käsittelyyn (esim. sähköiset asiakirjat ja niiden henkilöhakuiset kokoelmat). Malliesimerkkinä voidaan pitää RtsD:n 25 artiklassa tarkoitettuja ns. lokitiedot, joilla voidaan ymmärtää tietyn tietojärjestelmän pääsyn- ja käytönvalvonnan tarkoituksissa kerättävinä käyttäjätietoina. Ne ovat henkilötietoja monestakin näkökulmasta (tietyn käyttäjän käsittelemät mahdollisesti monia henkilöitä koskevat tiedot). Niihin voidaan soveltaa julkisuuslakia (ks. KHO 2014:69) ja ne ovat merkittävä näyttö henkilötietojen oikeudetonta käsittelyä tutkittaessa ja käsiteltäessä tuomioistuimessa.

2 luku Henkilötietojen käsittelyn yleiset edellytykset

Kun EU:n uudistus perustuu periaatepohjaiseen sääntelyyn, on mielestäni nimenomaan kansallisessa yleislaissa esitettävä nämä periaatteet ja silloin periaatteet olisi hyvä mainita jo luvun otsikossa. Kun periaatteita voidaan pitää tietosuojaoikeudellisten yleisten oppien perusteena, olisi perusteltua esittää ne myös tiivistetysti kuten RtsD:n 4 artiklassa. Ehdotuksen esitystapa hajottaa nämä kuusi periaatteetta vaikeasti hahmotettaviksi ilman direktiivin rinnakkaista luentaa. Esimerkiksi 2. luvussa ei esitellä kuudetta periaatetta (tietoturva)

siten kuin se ilmenee RtsD:n 4.1 e) kohdassa vaan tuodaan erikseen esille omassa 5. luvussa.

4 § Laillisuusvaatimus

Kyse on lainmukaisuus -periaatteesta, joka TsA:ssa viittaa henkilötietojen käsittelyperusteisiin ja vastaa perinteisesti kysymykseen kenen henkilön tietoja on oikeus käsitellä. Viranomaistoiminnassa tällä periaatteella on myös yleisempi viranomaistoiminnan laillisuusvaatimuksesta johdettavissa oleva merkitys. Tässä yhteydessä kyse ei ole henkilötietolain 5 §:n verrattavissa olevasta huolellisuusvaatimuksesta, mihin pykälän perustelut viittaavat vaan henkilötietolain 8 §:n 4 kohdan ja 12 §:n 5 kohdan käsittelyperusteista. Henkilötietolain 5 §:ä vastaavat RtsD:n säännökset ovat lähinnä 19 ja 20 artiklat.

Ehdotuksen mukaan lainmukaisuuden periaate täyttyy vain, jos käsittelystä säädetään laissa. Perustelujen mukaan jää epäselväksi, voisiko ehdotettu laki sellaisenaan olla tällainen säännösperuste vai edellyttääkö laillisuusvaatimuksen täyttäminen aina muuta lakitasoista ja nimenomaan käsittelysäännöstä, jolloin lakisääteinen tehtäväsäännös ei yksistään riittäisi. RtsD:n 8.1 artiklassa lähdetään viranomaisen tehtävästä, jonka suorittamiseksi henkilötietojen käsittely on tarpeellista. Asiaan vaikuttaa tietysti henkilötietojen suojan perusoikeuden tulkinta erityisesti EU:n tietosuojauudistuksen jälkeen, vaikka RtsD antaisi ymmärtää johdanto-osan 33 kohdassa, ettei direktiivin viittaukset jäsenvaltion lainsäädäntöön välttämättä edellytä parlamentissa hyväksyttyjä säännöksiä.

5 § Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuuden periaate on keskeisin tietosuojaperiaate, koska se lisää käsittelyn ennakoitavuutta rajoittamalla käsittelyn nimenomaisiin ja laillisiin tarkoituksiin kuten RtsD:n 4.1 b) artiklassa tämä periaate ilmaistaan sekä rajaa kokonaisuudessaan käsittelyn elinkaarta. Tätä keskeistä periaatetta ei voi jättää sen varaan, miten rekisterinpitäjä on sen kulloinkin määrittelyt tai jättänyt määrittelemättä.

Käyttötarkoitussidonnaisuuteen perustuvan sääntelyn kaksi keskeistä kysymystä ovat: 1) miten alkuperäinen (ensisijainen) käsittelytarkoitus ja sen rajat voidaan määritellä ja tunnistaa, jotta se voisi toimia luontevasti yhteensopivuusarvioinnin perusteena ja 2) miten tunnistetaan tilanteet, joissa ei ole enää kyse yhteensopivasta käsittelystä, mutta käsittelyyn liittyy sellaisia intressejä, joiden perusteella voitaisiin käyttötarkoitussidonnaisuuden periaatteesta joustaa (toissijainen käsittely) tai siitä nimenomaan poiketa. TsA:ssa yhteensopivuusarvioinnista ja käyttötarkoituksesta poikkeamisen edellytyksistä säädetään 6.4. artiklassa, mihin RtsD:n 9.1 artikla näyttäisi nimenomaan viittaavan.

Jotta käyttötarkoitussidonnaisuus olisi selkeä käsittelyä ohjaava periaate, on käyttötarkoitus johdettava käsittelykohtaisesti useimmiten käsittelyn oikeudellisesta perusteesta, joka on näissä tilanteissa viime kädessä viranomaisen lakisääteiset tehtävät. Vaikka ehdotuksen 4 §:n mukaan käsittelystä tulisi säätää laissa eikä viranomaisen lakisääteinen tehtävä sellaisenaan riittäisi käsittely perusteeksi (vrt. TsA 6.1 c) ja e) kohdat), voidaan katsoa, että yksityiskohtaisemmat käsittelysäännöksetkin perustuvat arvioon, joka tehdään lakisääteisten tehtävien edellyttämän käsittelyn perusteella. Tämän perusteella ehdotan,

että ehdotuksen 5 §:n 1 momenttiin lisättäisiin määrite ”...ja laillisia...” kuten RtsD 4.1 b) artiklassa ja se viittaisi viime kädessä viranomaisen lakisääteisiin tehtäviin ja yleisemmin viranomaistoiminnan lainalaisuusvaatimukseen myös henkilötietojen käsittelyn osalta.

Ehdotuksen 5 §:n 2 momentti liittyy edellä mainittuun toissijaiseen käsittelyyn tai käyttötarkoituksesta poikkeamiseen, mikä edellyttää tällaisten tilanteiden tunnistamista. Perinteisessä ja voimassaolevassa salassapitoperusteisessa sääntelyssä nämä kysymykset on ratkaistu salassapitosäännökset syrjäyttävillä tiedonsaantia tai tiedonantamista koskevilla säännöksillä, minkä takia tässä yhteydessä tulisi kansallisesti arvioida miten nämä erilaiset sääntelykeinot voitaisiin yhteen sovittaa.

Lisäksi ehdotuksen 5 §:n 2 momentti viittaa ehdotuksen koko 1 §:n, jolloin jää epäselväksi, mikä on ehdotuksen 1 §:n 1 momentin ja 2 momentin tehtävien ja käyttötarkoitusten keskinäinen suhde. Edellä mainittu huomioon vaihtoehtoja on kolme eli käsittely voi olla **yhteensopivaa**, vaikka tietoja luovutettaisiin, käsittelytarkoituksesta voidaan joustaa ns. **toissijaista käsittelyä koskevan sääntelyn perusteella** tai kyse olisi **erikseen säädetyistä poikkeuksista käyttötarkoitussidonnaisuudesta**. Ottaen lähtökohdaksi RtsD:n 9.1 artiklan tulisi ehdotuksen 1 §:n 1 momentin ja 2 momentti eriyttää siten, että kussakin kohdassa kyse on eri käyttötarkoituksista, jolloin keskinäisistä käyttötarkoituspoikkeuksista voitaisiin tarvittaessa säätää erityislaeissa.

Ehdotuksen 5 §:n 3 momentti liittyy RtsD 4.3 artiklaan, joka koskee vain ehdotuksen 1 §:n 1 momentin käsittelyä. Direktiivi näyttäisi näiltä osin viittaavan TsA:n 5.1 b) (käyttötarkoitussidonnaisuus) ja e) (säilytyksen rajoittaminen) kohdissa tarkoitettuihin yleisen edun mukaisiin käsittelytarkoituksiin kuten arkistointi, tieteellinen tai historiallinen tutkimus sekä tilastointi. Ottaen huomioon RtsD:n 9.2 artikla, säännöstä ei voida sellaisenaan pitää itsenäisenä käsittelyperusteena ehdotuksen 1 §:n 1 momentissa toimivaltaiselle viranomaiselle käsitellä henkilötietoja tällaisissa toissijaisissa tarkoituksissa, ellei tällaista käsittelyperustetta voida johtaa TsA:sta tai siihen perustuvan kansallisen liikkumavaran puitteissa annettujen säännösten perusteella kuten yleisen edun arkistointitarkoitukset, tieteellinen tutkimus ja tilastointi. Tästä syystä säännöstä voidaan pitää lähinnä viittauksena TsA:n 89.1 artiklassa säädettyihin rekisteröidyn oikeuksia ja vapauksia koskeviin asianmukaisiin suojatoimiin.

6 § Tarpeellisuusvaatimus

Ehdotuksen 6 §:ssä on käsitelty kahta tietosuojaperiaatetta, mikä voi helposti johtaa niiden sekaantumiseen. Ensimmäinen momentti koskee käsiteltävien henkilötietojen tarpeellisuutta, mikä viittaa RtsD 4.1 c) kohdan tarpeellisuus -periaatteeseen. Perinteisesti tällä on tarkoitettu sitä, mitä tietoja yksittäisestä rekisteröidystä kerätään niiden minimoinnin tarkoituksessa, kun rekisteröityjen piiri (ketkä henkilöt) on ensin lainmukaisuus -periaatteen nojalla ratkaistu.

Toinen ja kolmas momentti koskevat tarpeellisuutta käsittelytarkoituksen kannalta, mikä liittyy useimmiten käsittelyn kokonaiskestoon eli periaatteeseen, joka ilmaistaan RtsD 4.1 e) kohtaa yleisemmin TsA 5.1 e) kohdassa säilytyksen rajoittamisen periaatteena. Tämä säilyttämisen rajoittamisen -periaate kohdistuu ensisijaisesti käsittelyn henkilölliseen laajuuteen (onko tiettyä henki-

löä koskevia tietoja enää tarpeen käsitellä). RtsD:ssä tämä periaate on kirjattu 4.1 e) kohtaan hyvin keino-orientoituneesti viitaten aineiston käsittelyyn siten, ettei rekisteröity ole enää tunnistettavissa, kun tiedot eivät ole enää käsittelytarkoituksen kannalta tarpeellisia. Tietysti vaihtoehtona tulisi olla myös tietojen tietoturvallinen hävittäminen varsinkin, jos aineiston anonymisointi ei onnistu tai aineisto ei enää anonymisoituna ole edellä mainituissa toissijaisissa käyttötarkoituksissa käyttökelpoinen.

Kolmas momentti liittyy RtsD:n 5 artiklaan, joka viittaa säännöllisin väliajoin tehtävään henkilötietojen säilyttämisen tarpeellisuuden arviointiin. Tässä yleislaissa säännöstä voidaan pitää perusteltuna, kunhan erityissäännöksissä esitellään ja otetaan käyttöön tehokkaita keinoja tämän periaatteen toteuttamiseksi kuten esimerkiksi enimmäissäilytysaikasäännökset ja automatisoitu poisto ja tällaisen enemmän tai vähemmän mekaanisen enimmäisaikasääntelyn ohella riskiperusteinen arviointi säilyttämisajoista esim. kansallisen turvallisuuden perusteella käsiteltävistä henkilötiedoista.

Konkreettisesti tämä kahden periaatteen käsittely samassa pykälässä johtaa epäjohdonmukaisuuteen ehdotuksen 25 §:ssä tarkoitettujen erityisesti rekisteröityjen poistovaatimusten osalta. RtsD 16.2 artiklan mukaan poistovaatimus olisi tehokas, jos tietojen käsittely rikkoo 4, 8 ja 10 artiklan nojalla annettuja säännöksiä. Sen sijaan 5 artiklan nojalla annettuihin säännöksiin ei voisi direktiivin mukaan yksittäisessä tapauksessa vedota. Ehdotuksen 25 §:n 2 momentti kattaa 6 §:n kokonaisuudessaan, jolloin yksittäinen poistovaatimus voisi perustua myös 5 artiklan nojalla annettuun 6 §:n 3 momenttiin. Sinänsä en pidä tätä puutteena vaan enemmänkin rekisteröityjen yhdenvertaisuuskysymyksenä eli jos säännönmukaista säilyttämisaikaa arvioidaan yksittäisen vaatimuksen osalta uudestaan ja tällainen vaatimus hyväksytään, tulisi rekisterinpitäjän ryhtyä oma-aloitteisesti toimenpiteisiin henkilötietojen poistamiseksi muidenkin vastaavissa tilanteissa olevien rekisteröityjen osalta ja varsinkin silloin kuin poisto perustuu enimmäissäilytysaikojen ylitykseen.

Ehdotan näiden kahden periaatteen erottamista eri pykäliin.

7 § Virheettömyysvaatimus

RtsD:n 4.1 d) kohdassa ei enää puhuta niinkään tietojen virheettömyydestä vaan realistisemmin tietojen täsmällisyydestä ja tarvittaessa ajantasaisuudesta sekä kohtuullisista toimenpiteistä käsittelyn tarkoituksiin nähden virheellisten tietojen poistamisesta tai oikaisemisesta. Ehdotan säännökseen ainakin lisättäväksi määrite täsmällisiä siten, että virheettömyyttä ja täsmällisyyttä arvioidaan suhteessa käsittelyn tarkoitukseen. Yksittäiset tiedot voivat olla virheettömiä, mutta siitä huolimatta ne voivat olla käyttötarkoituksen kannalta epätäsmällisiä.

Henkilötietolaissa säännös on sijoitettu 9 §:n, jonka otsikkona on tietojen laatua koskevat periaatteet. Kun periaatteet oikeusnormeina eivät ole joko/tai vaan enemmän/vähemmän sovellettavia sääntöjä, on henkilötietolain virheettömyysvaatimus suhteellisuusperiaatteineen malliesimerkki voimassaolevasta tietosuojaperiaatteesta.

RtsD:ssä suhteellisuusperiaate ilmaistaan yleisesti ja kattavasti 20 artiklassa. Kyse ei ole vain suojaustoimenpiteiden riskiperusteisesta arvioinnista vaan kaikkien tietosuojaperiaatteiden tehokkaasta toteuttamisesta käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä. Vaikka ehdotuksen 15 §:n otsikko on yhteneväinen RtsD:n 20 artiklan kanssa, on se sisällöltään enemmänkin voimassa olevan henkilötietolain 32 §:n suojausvelvoitteeseen sisältyvän suhteellisuusperiaatteen ilmentymä kuin 20 artiklan mukaisesti kaikki tietosuojaperiaatteet kattava säännös.

Ehdotuksen 7 § ei sisällä erityistä suhteellisuusperiaatetta eikä edellä mainitun perusteella ehdotuksen 15 § kata henkilötietojen täsmällisyyteen liittyvää suhteellisuusperiaatetta. Ottaen huomioon erityisesti johdannossa esitellyt kaksi ensimmäistä käsittelytyyppiä, joissa henkilötietojen käsittelyyn ryhdytään hyvin täsmentymättömien tietojen varassa pyrkien laillisten tiedonhankintakeinojen avulla täsmentämään ja varmistamaan tietoja, tulisi suhteellisuusperiaate ilmaista myös lakitekstissä eikä vain perusteluissa ja siten kuin se riskiperusteisenä lähtökohtana RtsD:n 20 artiklassa ymmärretään kattaen kaikki tietosuojaperiaatteet.

Asiallisesti tämän tietojen täsmällisyys -periaatteen alaan kuuluu myös RTSD 7 artikla. Säännös näyttäisi perustuvan metadata -tyyppiseen erotteluun sen mukaan onko henkilötieto jotenkin faktaperusteinen vai onko se henkilökohtaiseen arvioon perustuva tieto. Erityisenä soveltamistilanteena riskiperusteisen lähtökohdan mukaisesti säännöksessä tunnistetaan tietojen luovuttamistilanteet, joiden kautta virheellisillä tai epätäydellisillä tiedoilla voi olla olennainen vaikutus henkilön suojattaviin oikeuksiin tai vapauksiin.

8 § Eräiden henkilötietojen erottaminen toisistaan

Ehdotuksen 8 §:n 1 momentti liittyy RtsD:n 6 artiklan kansalliseen voimaansaattamiseen. Artiklateksti on ehdotusta informatiivisempi, koska se yksilöi luonnollisten henkilöiden erilaisia rooleja käsiteltäessä henkilötietoja rikosasioiden tarkoituksissa ja konkretisoi omalta osaltaan näihin rooleihin liittyviä erilaisia yksilöiden suojattavia oikeuksia ja vapauksia, joita käsittely voi vaarantaa. Tällaista roolierottelua voidaan pitää olennaisena tietosuojaa koskevan vaikutusarvioinnin kannalta.

Näistä syistä ehdotan, että säännöksessä yksilöidään ”eri asemassa olevat rekisteröidyt” kuten RtsD:n 6 artiklan a) – d) kohdissa.

11 § Erityisiä henkilötietoryhmiä koskeva käsittely

Tämän säännöksen osalta viitataan henkilötietolain 11 §:n ja nimetään nämä tiedot arkaluonteisiksi tiedoiksi lukuun ottamatta rikosta tai sen seuraamuksia koskevia tietoja. Tässä yhteydessä olisi syytä harkita sitä, onko kansallisesti tarpeen enää nimetä näitä tietojen arkaluonteisiksi tiedoiksi, kun nimitystä ei enää käytetä TsA:ssa eikä RtsD:ssä vaan kyse on lähinnä riskiperusteisessa lähestymistavassa huomioitavista seikoista RtsD:n 19, 20, 27 ja 29 artikloissa tarkoitetuissa arvioinneissa.

Jotkut rikostyypit ovat luonteeltaan sellaisia, että niiden tutkinnassa käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja kuten rotua, etnistä alkuperää, ter-

veydentilaa tai seksuaalista käyttäytymistä koskevia tietoja. Tällaisten oikeudenloukkausten tutkinnan kannalta näitä tietojen voi pitää ehdottoman välttämättöminä ja ilmeisesti käsittelyn voi katsoa perustuvan ehdotuksen 11 §:n 2 momentin 1 kohtaan ja lakisääteinen peruste olisi erityisesti esitutkintalaki.

12 § Henkilötunnuksen käsittely

Henkilötunnuksen käsittelyssä tulisi korostaa sitä, että sen perinteinen funktio on toimia henkilötiedollisena tunnisteena tai erotteluvälineenä ja tässä tarkoituksessa se parantaa tietojen laatua (vältetään samannimisten henkilöiden tietojen sekaannukset). Sen sijaan sitä ei pidä käyttää yksistään henkilön tunnistamisen välineenä, jossa se muodostaa merkittävän riskin kuten identiteettivarkaustyyppinen henkilötietojen väärinkäyttö.

Edellä 5 §:n 3 momentissa lausutun perusteella henkilötunnuksen käsittely historiallista tai tieteellisestä tutkimuksesta taikka tilastointia varten määräytyy TsA:n mukaan, minkä takia ehdotan ehdotuksen 12 §:n 1 momentin 3 kohdan poistamista.

14 - 15 § Rekisterinpitäjän vastuu ja sisäänrakennettu ja oletusarvoinen tietosuoja

Ehdotettu 14 § perustuu RtsD:n 19 artiklaan, joka yhdessä 20 artiklan kanssa muodostavat ns. riskiperusteisen lähestymistavan perusteet. Kyse ei ole vain käsittelyn lainmukaisuuden varmistamisesta ja osoittamisesta vaan kaikkien tietosuojaperiaatteiden tehokkaasta toteuttamisesta ottaen huomioon uusin tekniikka ja toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisen henkilön oikeuksille ja vapauksille. Kyse on myös kattavin suhteellisuusperiaatteen ilmentymä RtsD:ssä, mistä syystä ehdotan, että ehdotuksen 14 §:ä muutetaan vastaamaan 19.1 artiklan riskiperusteista lähestymistapaa.

Tällainen riskiperusteinen lähestymistapa olisi varsinkin kansallisessa yleislaissa perusteltu, koska yleislain perusteella tehtävä vaikutusten arviointi (RtsD 27 artikla ja erityisesti TsA 35.10) voisi yksilöidä tarpeelliset erityissäänntelyn kohteet mukaan lukien luovutussäännökset tai niitä korvaavat käsittelysäännökset.

17 § Henkilötietojen käsittelijä

Henkilötietojen käsittelijällä tarkoitetaan rekisterinpitäjän lukuun tapahtuvaa henkilötietojen käsittelyä. Ehdotuksen 17 §:n 2 momentti koskee vain tällaista käsittelijää. Ehdotan, että säännöksen lisätään RtsD:n 23 artiklasta ilmenevä muu käsittelijä, joka määritellään rekisterinpitäjän tai käyttäjän alaisuudessa toimivaksi henkilöksi, jolla on pääsy henkilötietoihin. Kyseessä on tyypillisesti palvelussuhteessa oleva käyttäjä ja säännöksen ulottaminen myös häneen on henkilörekisteririkos – tyyppisen rikosvastuun perusedellytys. Käyttäjien sitouttaminen salassapitovelvollisuuteen ei sellaisenaan riitä, kun on kyse viranomaistehtävissä annetuista käyttöoikeuksista ja niiden käytöstä muissa kuin laillisissa tarkoituksissa.

19 § Lokitiedot

Kuten perusteluissa todetaan yleisiä säännöksiä lokitiedoista ei ole, mikä nostaa esille tarpeen säädellä lokitietoja ja niiden käsittely yleisemmin. Kuten edellä esitin lokitiedot ovat tyyppiesimerkki henkilötietojen käsittelystä, johon voidaan ja tulee sovellettavaksi monet informaatio-oikeudelliset säännökset. Kun kyse on oikeutettua käyttäjää koskevasta käyttötiedon keräämisestä, on kyse henkilötietojen käsittelystä, johon itsessään on sovellettava tietosuojaoikeudellisia periaatteita.

Kun lokitietojen käsittelyssä on kyse ensisijaisesti rekisterinpitäjän oma valvonnasta kuten RtsD:n 25.2 ilmenee, ei tarkkaan ottaen ole kyse RtsD:n soveltamisalaan kuuluvasta käsittelystä vaan TsA:n soveltamisalaan kuuluvasta käsittelystä. Tämä nostaa esille yleisemmin tarpeen säädellä lokitietojen käsittelyä yleisessä tietosuojalaissa (ns. Tatti-laki). TsA:n käsittelyperusteista voisi tässä tapauksessa tulla kyseeseen 6.1 c) kohdan lakisääteisen velvoitteen noudattaminen. Tässä tapauksessa tällainen velvoite on johdettavissa rekisterinpitäjän henkilötietolain 32 §:n suojausvelvollisuudesta, joka ilmenee RtsD:n 29 artiklasta sekä RtsD:n 30 artiklan edellyttämästä tietoturvaloukkauksien havaintokyvykkyyden varmistamisesta.

Lokitietoja koskeva RtsD:n 25 artikla näyttäisi ensisijaisesti koskevan sitä, mitkä käsittelytapahtumat olisi kirjattava ylös mukaan lukien käsittelijöiden tunnistamistiedot. Siihen, mihin säännös ei suoranaisesti ota kantaa, on se, mitkä tietojärjestelmät tai henkilötietojen käsittelyt on lokitettava. Ehdotuksen 19 § on tässä suhteessa yleisemmin ymmärrettävissä, mikä johtaa säännöksen soveltamisen kannalta kysymykseen eli onko kaikki RtsD:n alaan sekä ehdotuksen 1 §:n 2 momentin alaan kuuluva käsittely lokitettava.

Vastaus tähän kysymykseen näyttäisi muodostuvan lokituksen käsittelyperusteista eli RtsD:n 29 ja 30 artikloista, joissa varsinkin 29 artikla lähtee riskiperusteista arvioinnista, jossa 29.1 artiklan mukaan voidaan ottaa huomioon eri suuntiin vaikuttavia tekijöitä eli uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään vaihtelevat riskit. Näiltä osin ehdotan, että ehdotuksen 31 §:ä muutettaisiin vastaamaan RtsD:n 29.1 artiklan riskiperusteisen arvioinnin muotoilua kuten myöhemmin esitetään.

Lisäksi tulisi säätää lokitietojen saatavuudesta ja käsittelystä tilanteissa, joissa rekisteröity epäilee tietojensa luvatonta käsittelyä, mutta hän ei ole julkisuuslaissa tarkoitettu asianosainen eikä hänellä ole oikeutta lokitietoihin julkisuuslain perusteella (KKO 2014:69).

Ehdotan lisäksi 19 §:n siirtämistä ehdotuksen 32 §:n yhteyteen ja näiden säännösten em. yhteyden selventämistä perusteluissa.

20 § Tietosuojaa koskeva vaikutustenarviointi

Kyse on tietosuojauudistuksen keskeisestä itseohjauksellisesta työkalusta, joka tulee soveltamisen myötä kehittymään. Kynnys sen käyttämiseen ei tulisi olla kovin korkea. Lainsäädäntöperusteisen käsittelyn osalta olisi perusteltua

kirjata lainsäädäntöön se, että direktiivin alaan kuuluvassa lainvalmistelussa laaditaan siihen tarkoitukseen soveltuva vaikutusarvio, joka voitaisiin toimittaa valvontaviranomaiselle ehdotuksen 52 §:n 2 momentin kuulemisen yhteydessä.

Myös tässä säännöksessä käsittelyyn liittyvä riskiarvion kuvaus ”saattaa aiheuttaa merkittävän riskin luonnollisen henkilön oikeuksien toteutumiselle” on jäänyt olennaisesti suppeammaksi kuin RtsD:ssä ja sen 27.1 artiklassa. Kun RtsD:n 27.1. artikla vastaa muuttuvat muuttaen TsA:n 35.1 artiklaa, ei mielestäni ole mitään syytä eriyttää tätä arviointia asetuksen arvioinnista vaan pitää ne ainakin arviointiperusteiden osalta yhtenäisinä. Ehdotan, että myös näiltä osin sitä, että ehdotuksen riskiarviointikuvaus muutetaan vastaamaan RtsD:n 27.1 artiklassa esitettyä muotoilua.

Lisäksi ehdotan, että myös ehdotuksen 20 §:n 2 momentti tulisi vastata TsA:n 35.7 artiklaa arvioinnin dokumentoinnin vähimmäisvaatimuksista, jotta niitä voidaan joustavasti kehittää sen mukaan, onko kyse lainsäädäntövaiheen vai olemassa olevan käsittelyn arvioinnista.

4 luku Rekisteröidyn oikeudet

22 § Yleisesti saataville asetettava tietosuojaseloste

Ehdotuksen muotoilu kirjallisesta selosteesta ja sen julkistamisesta on vanhakantainen muotoilu, mikä viittaa hetkelliseen julkaisuun esimerkiksi virallisessa lehdessä. Otsikko viittaa yleisesti saataville asettamiseen, kun taas RtsD:n 13.1 artiklassa puhutaan rekisteröidyn saataville asettamisesta, mikä viittaisi jossain määrin kohdennetumpaan viestintään kuin esimerkiksi minne tahansa rekisterinpitäjän kotisivulle saataville asetettuun selosteeseen. Tämän takia ehdotan, että otsikko ja säännöstekstiä muutetaan siten, että seloste tulee asettaa rekisteröidyn saataville. Käytännössä tämä voisi tarkoittaa esimerkiksi selosteen sijoittamista kotisivuosioon, jossa kerrotaan rekisteröidyn oikeuksista.

23 § Rekisteröidyn tarkastusoikeus

Kuten voimassaolevan henkilötietolain 26 §:ssä edellytetään, tulisi tämäkin tarkastusoikeudeksi nimetty oikeus sisältää vahvistuksen myös siitä, ettei luonnollista henkilöä koskevia tietoja käsitellä. Tätä edellyttää myös RtsD:n 14 artikla. Lisäksi sääntelyn soveltamisalaan kuuluu lukuisia tietojärjestelmiä kuten rikosrekisteri, jonka osalta myös tieto siitä, ettei ole rekisteröity, on olennainen tieto ja siten sen kuuluu olla tarkastusoikeuden piirissä.

Kun tässä tarkoitettu tarkastusoikeus ei ole sidottu henkilörekisteriin, voi käsiteltävien tietojen antaminen edellytä niiden hakemista ja jos tarkastusoikeuden käyttäjää ei mitenkään avusteta pyynnön kohdentamiseen, voi tarkastusoikeuden käytöstä tulla hyvinkin työläs toimenpide rekisterinpitäjän näkökulmasta. Osittain varmaan tästä syystä RtsD:n 13.2 artiklassa on esitetty säädettäviksi rekisterinpitäjän velvoitteista, joilla rekisterinpitäjän tulee informoida erilaisista käsittelytyypeistä tai -tarkoituksista, jotta rekisteröity voisi käyttää oikeuksiaan. Tämä on ajateltu hoitaa ehdotuksessa 22 §:ssä tarkoitetulla tietosuojaselosteella ja ehdotuksen 30 §:n edistämisvelvollisuudella, jota tulisi terävöittää siihen suuntaa, että se auttaa rekisteröityä kohdistamaan tarkastusoikeuden haluamallaan tavalla.

RtsD:n 14 artiklan johdantolauseen ”oikeus saada pääsy henkilötietoihin” ei vaikuta enää pelkältä vastaukselta tarkastusoikeuspyyntöön tai jäljennökseltä käsiteltävistä henkilötiedoista vaan pääsyltä itse tietoihin sähköisen käyttöliittymän kautta. Sitä, miksi tällaista ”oikeutta saada pääsy henkilötietoihin” ei miltään osin esitetä, ei ole ehdotuksessa perusteltu. Toisaalta tällaista oikeutta ei tulisi poissulkea, jos tällaiseen pääsyn antamiseen on jo olemassa ja varmaan tulevaisuudessa yhä enemmän tulee olemaan teknisiä ratkaisuja.

Toinen RtsD:n 14 artiklan haaste liittyy siihen, että joiltakin osin annettavat tiedot ovat vakioisia ja joiltakin osin rekisteröity -kohtaisia. Tarkastusoikeus henkilötietolaissa koskee vain rekisteröityä koskevia tietoja, jos niitä ylipäänsä on. Henkilötietolain tarkastusoikeus ei ole koskenut sitä, kenelle henkilötietoja on luovutettu muuta kuin erityisesti säädetyissä tilanteissa kuten luottotietolain 30 §:n 2 momentti, mikä on yksi mahdollinen ratkaisu lokitietojen käsittelyyn. Tähän suuntaan on edetty muun muassa kansallisen terveysarkiston Omakanta.fi -palvelussa.

Ehdotuksen 23 §:n 1 momentin 4 kohdassa viitataan vastaanottajiin tai vastaanottajaryhmiin, joille rekisteröidyn henkilötietoja on luovutettu. Kun henkilötietolain 26 §:n tarkastusoikeuden osalta puhutaan vain tiedonantamisesta siitä, mihin tietojen säännönmukaisesti luovutetaan, on ehdotus ymmärrettävissä siten, että sen perusteella tulee antaa tiedot myös vastaanottajista, joille rekisteröidyn tiedot on luovutettu. Näiltä osin viittaus ehdotuksen 3 §:n 8 kohdan vastaanottajan määritelmään näyttäisi osittain johtavan siihen, ettei ehdotuksen 1 §:n 1 momentin tarkoituksessa tehdyistä luovutuksista tarvitse ilmoittaa, vaikka nekin tulisi lokittaa riskiperusteisen arvioinnin mukaisesti. Tämän jälkeenkin jää epäselväksi se, onko myös luovutettu tietosisältö ilmoitettava ja miten säännöstä tulisi soveltaa luovutettaessa tietoja ehdotuksen 1 §:n 2 momentin tarkoituksiin tai toisinpäin ottaen huomioon erilaiset salassapitointressit mahdollisina rajoitteina, koska ehdotukseen ei sisälly henkilötietolain 26 §:ssä mainittu salassapitosäännösten estämättä ehtoa.

24 § Tarkastusoikeuden rajoitukset

Ehdotuksen 24 §:n 1 momentissa säädetään tarkastusoikeuden lykkäämisestä, rajoittamisesta tai epäämisestä. Perinteisesti tarkastusoikeuden rajoitukset ovat tapauskohtaisesti arvioitavia, jolloin rajoituksen perusteena olevan oikeushyvän on katsottava siinä tilanteessa olevan vaarantumassa, jos tiedot annettaisiin. Ehdotuksessa käytetyt rajoitusten verbaaliset muodot (lykkäys, rajoitus tai epääminen) viittaavat ajalliseen, osittaiseen ja täydelliseen rajoittamiseen, mutta valinta niiden välillä tulisi kirjata säännökseen siten, että siitä ilmenee RtsD:n 15.1 artiklan kieltäytymisen välttämättömyyttä ja oikeasuhteisuutta suojattavan oikeushyvän osalta, jolloin rajoitus jäisi osittaiseksi tai ainakin ajallisesti rajatuksi.

Toinen perinteisesti tunnistettu tarkastusoikeuden rajoituksen muoto on ollut kategorinen, rekisterikohtainen rajoitus, joka ei edellytä tapauskohtaista arviointia. Esimerkkinä voidaan mainita PoreL:n (761/2003) 45 §:ssä mainitut tietojärjestelmät. Kyse voi olla täydellisen rajoittamisen muodosta, jota ei ehdotuksessa tarkemmin käsitellä ja siten tämän tyyppisestä rajoituksesta on säädettävä erikseen.

25 § Henkilötietojen oikaiseminen, poistaminen tai käsittelyn rajoittaminen

Säännöksellä on tarkoitus täytäntöön panna RtsD:n 16 artikla, jossa yhdistyy virheellisten tietojen oikaiseminen ja henkilötietojen poistoa tai rajoittamista koskevat vaatimukset. Erona näyttäisi olevan se, että 16.1 artikla koskee varsinaisia tiedollisia epätäydellisyys- ja virheväitteitä ja niiden oikaisemista tai täydentämistä. Sen sijaan 16.2 artikla koskee poistovaatimuksia silloin kun on ryhdytty asetuksen 4, 8 ja 10 artikloiden vastaiseen käsittelyyn, jolloin virheväitteet eivät ole useinkaan pääasiallisena perusteena vaatimuksille vaan 8 tai 10 artikloiden vastainen käsittely. Tällainen virhe- tai poistovaatimusten erottelu on jäänyt ehdotuksessa ja sen perusteluissa epäselväksi ja sitä tulisi ainakin perusteluissa selkeyttää.

Näiltä osin olisi myös nostettava esille erityissääntely, johon RtsD:n 18 artikla viittaa. Esimerkiksi kun esitutkinnassa epäiltyä kuullaan ja kuulemisesta laaditaan kuulustelukertomus, tulisi selvyyden vuoksi todeta, että näiltä osin sovelletaan esitutkintasäännöksiä ja jos epäilty haluaa muuttaa lausumaansa kyse ei ole tässä tarkoitetuista virheellisyys- tai epätäsmällisyysväitteiden käsittelystä vaan kuulustelukertomuksen muuttamisesta tai sen muuttamisesta oikeusprosessin seuraavassa vaiheessa.

Säännöksen toinen momentti liittyy poistovaatimuksiin, joiden menestyminen edellyttää sitä, että käsittelyssä on menetelty ehdotuksen 4 – 7 §:ien tai 11 §:n vastaisesti. Vastaava RtsD:n 16.2 artikla viittaa 4, 8 ja 10 artikloihin. Ehdotuksen 4 – 7 §:t sisältävät 4 artiklan periaatteista kaikki muut paitsi 4.1 f) kohdan eli tietoturva -periaatteen. Näiltä osin esitän viittausta myös tietoturva eli tietojen eheyden ja luottamuksellisuuden -periaatteisiin. Tämän perusteella poistamisen sijaan tietojen käsittelyä voitaisiin rajoittaa siten, että sijoitetaan tietojärjestelmän erityisesti suojattuun osaan kuten johdanto-osan 47 kohdassa esitetään.

26 § Rekisteröidyn vaatimuksen epääminen

Säännös ei niinkään koske epäämisen tai kieltäytymisen perusteita vaan sitä onko kieltäytymisen perusteista ilmoitettava rekisteröidylle. Kun ratkaisu voi olla myöskin se, että RtsD:n 18 artiklan perusteella sovellettavaksi ei tulekaan tässä tarkoitetut vaikuttamisoikeudet vaan kansallisesti rikostutkintaan ja rikosoikeudelliseen menettelyyn liittyvät erityissäännökset, tulisi tällaiset soveltamistilanteet selventää perusteluissa.

Säännöksessä ehdotetaan RtsD:n 16.4 implementoitavaksi siten, että kieltäytymisen perusteet voitaisiin jättää kertomatta säännöksessä mainituilla perusteilla, mutta kielteisestä päätöksestä sellaisenaan tulisi aina kertoa. Jos erityislainsäännössä on rajoitettu tiedollisia oikeuksia kategorisesti, tulisi tällaisessa erityissääntelyssä ottaa kantaa myös siihen, miten tässä tarkoitetut rekisteröidyn oikeudet toteutetaan.

5 luku Tietoturvallisuus

31 § Tietoturvallisuus

Ehdotuksessa riskiperusteisen lähtökohdan arviointikriteerit on kaikilta osin

mainittu, mutta kun kyse on kokonaisvaltaisesta riskiarvioinnista ja sen perusteella tehtävästä riskejä vastaavien suojauskeinojen valinnasta ja toteuttamisesta, voi esitystapa arviointikriteereiden jaottelusta ehdotuksen 1) – 4) kohdiksi hämärtää tämän säännöksen punnintaluonnetta. Ehdotan, että arviointikriteerit riskiperusteisessa säännöksessä kirjataan siten kuin RtsD:n 29.1 artiklassa.

32 § Henkilötietojen suojaaminen automatisoidussa käsittelyssä

Nämä RtsD:n 29.2. artiklassa esitetyt vaatimukset soveltuvat hyvin ilmiöön, joka tunnetaan kansallisesti teknisen käyttöyhteyden avaaminen tietojärjestelmään. Tekninen käyttöyhteys on julkisuuslaista ilmenevä käsite ja käytäntö, joka on laajasti levinnyt ja jota tulisi tässä yhteydessä arvioida yleisemmin.

Ehdotuksen monet yksittäiset kohdat voidaan ymmärtää tietojen käsittelyn lokitusta edellyttävinä säännöksinä.

35 § Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta rekisteröidylle

Näiltä osin esitän, että säännökseen lisätään RtsD:n 31.4 artiklan mukainen valvontaviranomaisen päätöstoimivalta.

8 luku Valvontaviranomainen

45 §. Tietosuojavirasto

Yleisenä huomiona totean, että valvontaviranomaista koskeva sääntelykokonaisuus jää tietosuojauudistuksen toimeenpanossa jokseenkin pirstaleiseksi, sillä nimenomaisesti Tietosuojavirastoa koskevia yleislain tasoisia säännöksiä sisältyy nyt lausunnon kohteena olevaan lakiin, ehdotettuun tietosuojalakiin ja yleiseen tietosuoja-asetukseen.

Ehdotetun lain 45 §:n 3 momentissa todetaan, että Tietosuojavirasto toimii riippumattomasti hoitaessaan tässä laissa säädettyjä tehtäviään. Riippumattomuuden joihinkin elementteihin on viitattu lain perusteluissa. Perusteluissa todetaan muun muassa: *Esimerkiksi 42 artiklan 5 kohtaa ei ehdoteta tässä laissa täytäntöön pantavaksi, sillä ehdotetussa tietosuojalaissa säädettäisiin Tietosuojaviraston henkilöstöstä ja siitä, että tietosuojavaltuutettu valitsee viraston henkilöstön.* Kuitenkin ehdotettu tietosuojalaki ei sisällä kyseistä säännöstä kokonaisuudessa. Ehdotettu tietosuojalain 8 §:n 2 momentissa todetaan, että *Tietosuojavirastossa on lisäksi esittelijöinä toimivia virkamiehiä ja muuta henkilöstöä*. Kyseisen tietosuojalain 8 §:n 2 momentin yksityiskohtaisissa perusteluissa taas viitataan TsA 52 artiklan 5 kohtaan, joka vastaa sisällöllisesti RtsD:n 42 artiklan 5 kohtaa.

Ehdotetun lain 45 §:n 3 momentin säännöstä tulisikin lain jatkovalmistelussa tarkastella suhteessa RtsD:n 42 artiklaan ja varmistua siitä, että kansallinen lainsäädäntö kattaa kaikki direktiivissä jäsenvaltioille asetetut velvollisuudet säätää valvontaviranomaisen riippumattomuudesta.[1] Henkilötietojen suojaa koskevan valvontaviranomaisen riippumattomuus on viranomaistoiminnan keskeinen elementti (esimeriksi perusoikeuskirjan 8 artiklan 3 kohta).

Kiinnitän huomiota, että ehdotettu tietosuojalaki ei tulisi kattamaan valvontaviranomaisen riippumattomuutta koskevia TsA:n 52 artiklan säännöksiä, koska 52 artikla ei varsinaisesti edellytä lainsäädännöllisiä toimenpiteitä. Lainsäätäjän tulisi arvioida, onko tällä faktisesti merkitystä, sillä kansallisen ehdotuksen mukaan Tietosuojavirasto valvoisi sekä TsA ja RtsD nojalla tapahtuvaa henkilötietojen käsittelyä.

47 §. Tietojensaantioikeus

Ehdotetun lain 47 §:n 1 momentissa säädettäisiin, että Tietosuojavirastolla on oikeus salassapitosäännösten estämättä - - muut tehtäviensä hoitamiseksi *välttämättömät* tiedot.

Henkilötietolain 39 §:n 1 momentin säännöksessä tietosuojaviranomaisten tiedonsaantioikeus on sidottu tietojen tarpeellisuuteen eikä ehdotettu säännös vastaa sanamuodoltaan RtsD:n 47.1 artiklan säännöstä.[2] Säännöksen perusteluja tulisi täsmentää perustuslakivaliokunnan ratkaisukäytännön mukaisesti ja varmistua siitä, ettei muutos heikennä valvontaviranomaisen kykyä valvoa henkilötietojen suojaa koskevia säännöksiä. Asian selvitysvaiheessa on rekisteröidyn, rekisterinpitäjän ja henkilötietojen käsittelijän oikeusturvan kannalta välttämätöntä, että tietyssä yksittäisessä asiassa saadaan mahdollisimman kattava kokonaiskuva henkilötietojen suojan täytäntöön panemiseksi.

48 §. Oikeus tehdä tarkastuksia

Ehdotetun lain 48 §:n 1 momentin mukaan tarkastusta ei saa tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa. Säännöksen perusteluissa todetaan ainoastaan, että näiltä osin nykytila muuttuisi, sillä henkilötietolain 39 §:n 2 momentin mukaisesti tietosuojavaltuutettu on saanut toimittaa kotirauhan piiriin kuuluvassa tilassa tarkastuksen.

Perusteluissa ei ole arvioitu tämän muutoksen merkitystä henkilötietojen suojaa koskevien säännösten valvonnalle. Kiinnitän huomiota siihen, että henkilötietojen käsittely voi tapahtua myös sellaisessa paikassa tai tilassa, joka nauttii perustuslain 10 §:ssä tarkoitettua kotirauhan suojaa. Tällaiset tilanteet eivät välttämättä ole niin relevantteja nyt lausunnon kohteena olevan valvonnan kannalta kuin ne ovat yleisen tietosuoja-asetuksen valvonnan kannalta, mutta lainsäätäjän on otettava huomioon, että henkilötietojen käsittely ei ole digitaalisen luonteensa vuoksi sidottu tiettyyn paikkaan tai tilaan.

Henkilötietojen käsittelyn luonteesta johtuen lähtökohtana on pidettävä, että henkilötietojen suojan valvontatoimivaltuuksien ulkopuolelle ei tulisi rajata tiettyä tilaa, kuten kotirauhan piriin kuuluvaa tilaa. Myös tällaisessa tilassa olisi, tiettyjen edellytysten täyttyessä, pystyttävä mahdollisimman laajasti valvomaan luonnollisten henkilöiden perusoikeuksien ja vapauksien toteutumista henkilötietoja käsiteltäessä.

Henkilötietojen käsittelyn luonteesta johtuen lähtökohtana on pidettävä, että henkilötietojen suojan valvontatoimivaltuuksien ulkopuolelle ei tulisi rajata tiettyä tilaa, kuten kotirauhan piriin kuuluvaa tilaa. Myös tällaisessa tilassa olisi,

tiettyjen edellytysten täyttyessä, pystyttävä mahdollisimman laajasti valvomaan luonnollisten henkilöiden perusoikeuksien ja vapauksien toteutumista henkilötietoja käsiteltäessä.

Pidän vähintään välttämättömänä, että lainsäätäjä arvio kyseisen muutoksen vaikutuksen valvontaviranomaisen tehokkaaseen kykyyn valvoa lausunnon kohteena olevan lain säännöksiä. Muutos on myös perusteltava.

49 § Asiantuntijan käyttö

Pykälän 1 momentin mukaan Tietosuojavirasto voi 48 §:ssä tarkoitetun tarkastuksen yhteydessä käyttää apunaan ulkopuolista asiantuntijaa. Myös näiltä osin kavennetaan nykytilaan, kun tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain (389/1994) 7 §:n mukaan tietosuojavaltuutetulla ja tietosuojalautakunnalla on oikeus kuulla asiantuntijoita sekä pyytää näiltä lausuntoja. Kyseisen säännöksen perusteluissa todetaan, että kyseistä voimassa olevan lainsäännöstä täsmennettäisiin, mutta perusteluissa ei oteta mitenkään kantaa siihen, että mahdollisuutta käyttää asiantuntijoita kavennettaisiin huomattavasti suhteessa nykytilaan.

Asiantuntijoiden käytöllä voi olla merkitystä myös muiden Tietosuojaviraston tehtävien hoitamisen kuin tarkastusten tekemisen kannalta. Tietosuojaviraston tehtäväkentän laajuudesta ja niukoista resursseista johtuen olisi oltava mahdollisuus selvittää asiantuntijan avulla myös muiden tehtävien hoitamisiksi, kuten rekisteröityjen oikeuksien toteuttamisessa taikka kuulemismenettelyissä. Myös arvioitaessa sitä, milloin henkilötieto voidaan katsoa anonyymiksi tiedoksi, voi edellyttää erityisasiantuntemuksen käyttämistä. Tietoturvan tason arvioiminen voi myös olla sellainen asia, jossa voi olla tarvetta konsultoida myös ulkopuolisia asiantuntijoita.

Katson, että Tietosuojavirastolla on oltava vastaava mahdollisuus käyttää asiantuntijoita kuin tietosuojaviranomaisilla on nykyisinkin.

50 §. Toimenpiteet (ja seuraamusjärjestelmä)

RtsD:n 47.2 artiklan mukaisesti kunkin jäsenvaltion on säädettävä tehokkaista korjaavista toimivaltuuksista. Kyseinen säännös sisältää esimerkinomaisen listauksen. RtsD:n täytäntöönpanossa on seuraamusjärjestelmän osalta päädytty ehdottamaan ratkaisua, jossa valvontaviranomaisen korjaavia toimivaltuuksia tehostettaisiin säätämällä oikeudesta määrätä uhkasakko päävelvoitteen koskevan määräyksen tehosteeksi.

Pykälän yksityiskohtaisissa perusteluissa todetaan, että pykälässä ehdotetaan Tietosuojavirastolle laajempia toimivaltuuksia, kuin mitä RtsD edellyttää. Kuitenkaan perusteluissa ei avata sitä, miten toimivaltuudet ovat laajemmat kuin, mitä RtsD edellyttää. Vaikuttaa siltä, että Tietosuojavirastolle säädettäisiin oikeus, nimenomaisesti RtsD:n 47.2 artiklan esimerkkilistauksen lisäksi, ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle tämän lain väitetystä rikkomisesta ja antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos tämä on käsitellyt henkilötietoja lainvastaisesti.

Perusteluissa ei tuoda esille arviota, jonka perusteella työryhmä on katsonut,

että ehdotetut toimivaltuudet ovat tehokkaita nyt lausunnon kohteena olevan lain säännösten toimeenpanemiseksi. Tämä on erityisen merkityksellistä siitä syystä, että toimivaltuuksien ”laajentamisella” perustellaan sitä, ettei esimerkiksi rekisterinpitäjään tai henkilötietojen käsittelijään kohdistuvista rikosoikeudellisista tai niihin verrattavista hallinnollisista seuraamuksista ole enää tarpeellista säätää.

Mietinnössä ei ole esimerkiksi arvioitu näiden korjaavien toimenpiteiden seuraamusluonnetta kansallisessa oikeusjärjestelmässä, saati sitten näiden säädettyjen korjaavien toimenpiteiden tehokkuutta, oikeasuhtaisuutta ja varoittavuutta seuraamuksina siten kuten RtsD:n 57 artikla edellyttää. Mietinnössä ei ole myöskään arvioitu sitä, miten nykyinen tietosuojalainsäädäntöä koskeva seuraamusjärjestelmä täyttäisi tehokkuuden, oikeasuhtaisuuden ja varoittavuuden kriteerit.

Esimerkiksi se seikka, että hallinnollinen seuraamusmaksu ei ole Suomen oikeusjärjestelmässä tavanomainen ratkaisu, ei ole peruste sille, että unionin oikeudessa asetettua velvoitetta säätää tehokkaasta, oikeasuhtaisesta ja varoittavasta seuraamusjärjestelmästä ei toimeenpantaisi ollenkaan. Unionin tietosuojauudistus edellyttää, että jäsenvaltiot vahvistavat säännöt tietosuojaa koskevien säännösten rikkomisten vuoksi määrättäviä seuraamuksia varten sekä toteutettavat kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhtaisia ja varoittavia.

Nyt ehdotettu ratkaisu on seuraamusjärjestelmä kokonaisuutena arvioiden riittämätön ja puutteellinen oikeusturvan, sääntelyn uskottavuuden ja nimenomaisten kansallisesti velvoittavien EU-oikeuden säännösten kannalta. Asiaa tarkasteltaessa on otettava huomioon tietosuojauudistuksen tarkoitus ja seuraamusjärjestelmä kokonaisuudessaan. Kiinnitän oikeusministeriön huomiota myöhemmin esitettäviin perusteluihin ja esitän kokonaisvaltaista arviointia, jossa esitetyt seikat otetaan asianmukaisesti huomioon.

Tietosuojavaltuutetun toimisto on toimittanut työryhmän sihteeristölle 28.9.2017 päivätyn muistion asiasta, joka on nyt tämän lausunnon liitteenä (liite 1). Keskeisinä huomioina nostan esille:

1) seuraamusjärjestelmää on tarkasteltava kokonaisuutena;

2) seuraamusjärjestelmä on kansallisesti sitovien EU-velvoitteiden nojalla pakollinen;

3) kyse ei ole ainoastaan siitä, voidaanko viranomaisille määrätä hallinnollisia sakkoja vaan kokonaisuudessa seuraamusjärjestelmän olemassa olosta ja tietosuojasääntelyn tehokkaasta toimeenpanosta siten kuin EU-oikeus siihen jäsenvaltioita velvoittaa. Jos kansallisesti päädytään siihen, ettei viranomaisille voida määrätä hallinnollisia sakkoja (ml. tiettyyn euromäärään alennetut sakot), on lainsäätäjän tehtävänä varmistua tehokkaan, varoittavan ja oikeasuhtaisen seuraamusjärjestelmän olomassa olosta ja sen täytäntöönpanosta;

4) tilanne, jossa seuraamus kohdistuu vain laiminlyönnin korjaamiseen, ei vastaa direktiivissä ja asetuksessa säädettyjä edellä esitettyjä reunaehtoja seuraamusjärjestelmälle, koska muutoin lainvastainen henkilötietojen käsittely jäisi ainakin tietyiltä osin kokonaan pakollisen seuraamusjärjestelmän ulkopuolelle.

53 §. Keskinäinen avunanto

Tässä yhteydessä tulisi varmistaa, että salassapito- tai muu sääntely ei aiheuta esteitä ylikansalliselle viranomaisyhteistyölle. Kyseisestä pykälästä tai sen perusteluista ei käy ilmi, miten tässä yhteydessä on arvioitu esimerkiksi salassapitoa koskevien säännösten vaikutusta valvontaviranomaisten keskinäisen avunannon toteuttamiseen.

56 §. Kantelun käsitteleminen

Ehdotuksen 56 §:n 1 momentin mukaisesti tietosuojaviraston on tutkittava kantelu sekä ilmoitettava sen tekijälle asian käsittelemisen etenemisetä ja sen tuloksista kohtuullisen ajan kuluessa. Hallintolain (434/2003) 23 §:ssä on viranomaisille säädetty velvollisuus käsitellä asia ilman aiheetonta viivytystä ja viranomaisen on esitettävä asianosaiselle tämän pyynnöstä arvio päätöksen antamisajankohdasta sekä vastattava käsittelyn etenemistä koskeviin tiedusteluihin.

Kansallisen hallintolain näkökulmasta on jokseenkin epäselvää, mistä erityinen vaatimus ”kohtuulliselle ajalle tulee” ja, miksi erityissäännös on tarpeellinen. Vaikuttaa siltä, että ehdotetulla pykälällä asetettaisiin Tietosuojavirastolle velvollisuus ilman erityistä pyyntöä informoida vireille saattajaa asian etenemisestä. RtsD 52.4 artiklan mukaan toimivaltaisen valvontaviranomaisen on ilmoitettava rekisteröidyllä valituksen etenemisestä ja ratkaisusta, mukaan lukien 53 artiklan mukaisten oikeussuojakeinojen mahdollisuudesta. Nämä sisältyvät jo hallintolain 23 §:än.

Lain jatkovalmistelussa tulisi arvioida RtsD 52.4 artiklan ja ehdotetun 56 §:n 1 momentin suhdetta hallintolain 23 §:än ja arvioida ehdotetun säännöksen tarpeellisuutta tästä näkökulmasta.

59 § Rikoslain rangaistussäännökset

Ehdotuksen 59 §:ssä on ainoastaan viittaus rikoslain säännöksiin ja siihen, että rikoslain 38 luvun 9 §:n henkilörekisteririkoksen yksityiskohtaiset muutokset valmistellaan TsA:n kansallisen täydentävän sääntelyn valmistelun yhteydessä. Näistä ns. Tatti-työryhmän ehdottamista muutoksista henkilörekisteririkoksen tunnusmerkistöön, olen lausunut työryhmän ehdotuksesta laaditussa lausunnossa 8.9.2017.

Tässä yhteydessä nostan esille kaksi näkökohtaa, jotka ovat henkilötietojen suojan ja erityisesti rikosoikeudellisen vastuun kannalta olennaisia. Ensinnäkin viranomaistoiminnassa säännösten vastainen henkilötietojen käsittely, jollei se täytä virkasalaisuuden rikkomisen tunnusmerkistöä, tulee useimmiten arvioiduksi virkavelvollisuuksien rikkomisena (ks. KKO 2014:86). Kyse ei ole vain vaitiolovelvollisuudesta vaan oikeudettomasta henkilötietojen käyttöoikeuksien käytöstä muihin kuin laissa säädettyihin tarkoituksiin. Tämä liittyy edellä 17 §:ssä esitettyihin muutosehdotuksiin, kun oikeuskäytännön mukaan yksittäinen käyttäjä voi myös syyllistyä henkilörekisteririkokseen.

Toinen näkökohta, joka jää usein yksittäistä käyttäjää koskevissa tapauksissa selvittämättä, on rekisterinpitäjän rikosoikeudellinen vastuu. Tyypillinen tekotapa olisi koko tietojenkäsittelyjärjestelmää koskevan suojauksen laiminlyönti,

joka edellyttää voimassaolevan tunnusmerkistön mukaan törkeätä huolimattomuutta. Jos suojauksen laiminlyönti on johtanut salassa pidettävien tietojen paljastumiseen, voisi toisena vaihtoehtona olla virkasalaisuuden tuottamuksellinen rikkominen. Mikäli RtsD:n 57 artiklan tarkoittamina seuraamuksina tullaan esittämään rikosoikeudellisen vastuun seuraamuksia, tulisi virkarikosvastuun säännöksiä rikosoikeudellisen laillisuusperiaatteen varmistamiseksi kehittää siten, että viranomaisen rekisterinpitäjänä tekemiin lainvastaisuuksiin tai laiminlyönteihin voitaisiin myös puuttua rikosoikeudellisin keinoin.

Tietosuojavaltuutettu Reijo Aarnio

Ylitarkastaja Heikki Partanen

LIITE 1 Tietosuojavaltuutetun toimiston muistio Seuraamusjärjestelmä 28.9.2017

---

[1] RtsD:n 42 artiklan 2 kohdan mukaan jäsenvaltioiden on säädettävä siitä, että niiden valvontaviranomaisten jäseneen tai jäseniin ei vaikuteta ulkopuolelta suoraan eikä välillisesti näiden hoitaessa tehtäviään käyttäessään valtuuksia tämän direktiivin mukaisesti, ja että ne eivät pyydä eivätkä ota ohjeita miltään taholta. Lisäksi kyseisen artiklan 4 kohdan mukaan kunkin jäsenvaltion on säädettävä siitä, että jokaiselle valvontaviranomaiselle osoitetaan tekniset, taloudelliset ja henkilöstöresurssit, tilat ja infrastruktuuri, jotka ovat tarpeen, jotta valvontaviranomaiset voivat suorittaa tehtävänsä ja käyttää valtuuksiaan tehokkaasti, mukaan lukien tehtävät ja valtuudet, jotka liittyvät keskinäiseen avunantoon, yhteistyöhön ja osallistumiseen tietosuojaneuvoston toimintaan. Lisäksi kyseisen artiklan 5 kohdan mukaan kunkin jäsenvaltion on säädettävä siitä, että jokaisella valvontaviranomaisella on oma henkilöstö, jonka se valitsee itse ja joka toimii kyseisen valvontaviranomaisen jäsenen tai jäsenten yksinomaisessa ohjauksessa. Lisäksi kyseisen artiklan 6 kohdan mukaan jokaisen jäsenvaltion on säädettävä siitä, että jokaiseen valvontaviranomaiseen sovelletaan varainhoidon valvontaa, joka ei vaikuta sen riippumattomuuteen, ja että sillä on erillinen ja julkinen vuotuinen talousarvio, joka voi olla osa valtion tai kansallista kokonaistalousarvioita.

[2] RtsD 47 artiklan 1 kohdan mukaan - - Näihin valtuuksiin on sisällyttävä vähintään valtuudet saada - - pääsy kaikkiin tietoihin, jotka ovat tarpeen valvontaviranomaisen tehtävien suorittamisessa.

Oikeusministeriö

Rikosasioiden tietosuojadirektiivin kansallisessa täytäntöönpanolaissa ollaan päätymässä esitykseen, jonka mukaan direktiivin edellyttämä seuraamussäännöksen ja niiden tehokas täytäntöönpano ehdotettaisiin toteutettavaksi siten, että valvontaviranomaisen korjaavia toimivaltuuksia vahvistettaisiin oikeudella määrätä uhkasakko korjaavan toimivallan käyttöä koskevan määräyksen tehosteeksi.

Sekä tietosuoja-asetus että tietosuojadirektiivi edellyttävät, että jäsenvaltiot vahvistavat säännöt tietosuojaa koskevien säännösten rikkomisten vuoksi määrättäviä seuraamuksia varten sekä toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhtaisia ja varoittavia.

Pidän tätä ratkaisua mahdollisen henkilötietojen käsittelyyn liittyvän virheen korjaamiseksi perusteltuna, mutta se on seuraamusjärjestelmä kokonaisuutena arvioiden riittämätön ja puutteellinen oikeusturvan, sääntelyn uskottavuuden ja nimenomaisten kansallisesti velvoittavien EU-oikeuden säännösten kannalta. Asiaa tarkasteltaessa on otettava huomioon tietosuojauudistuksen tarkoitus ja seuraamusjärjestelmä kokonaisuudessaan. Kiinnitän oikeusministeriön huomiota myöhemmin esitettäviin perusteluihin ja ohjaa arvioimaan asiaa kokonaisvaltaisesti ja niin, että esitetyt seikat otetaan asianmukaisesti huomioon.

Esittämäni huomiot koskevat yleisesti julkisen sektorin toimijoihin kohdistettavia seuraamuksia. Viittaan myös aiemmin TATTI-työryhmän mietinnön yhteydessä lausumaani rikoslakiin ehdotetuista muutoksista.

1. Asian kannalta merkitykselliset muut säännökset ja ehdotukset

Tietosuoja-asetuksen 83 artiklan 7 kohta

> Kukin jäsenvaltio voi asettaa sääntöjä siitä, voidaanko viranomaisille ja julkishallinnon elimille määrätä kyseissä jäsenvaltiossa sakkoja ja missä määrin, sanotun kuitenkaan rajoittamatta 58 artiklan 2 kohdan mukaisia korjaavia toimivaltuuksia.

Tietosuoja-asetuksen 84 artikla

> 1. Jäsenvaltioiden on vahvistettava säännöt tämän asetuksen rikkomisten vuoksi määrättäviä seuraamuksia varten, erityisesti niiden rikkomisten osalta, joihin ei 83 artiklan nojalla sovelleta hallinnollisia sakkoja, sekä toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Tällaisten seuraamusten on oltava tehokkaita, oikeasuhtaisia ja varoittavia.

2. Jäsenvaltioiden on toimitettava komissiolle 1 kohdan nojalla antamansa säännökset tiedoksi viimeistään 25.5.2018 ja niiden mahdolliset muutokset mahdollisimman pian.

Rikosasioiden tietosuojadirektiivin 57 artikla

Jäsenvaltioiden on vahvistettava säännöt tämän direktiivin nojalla annettuihin säännöksiin kohdistuvien rikkomisten johdosta määrättävistä seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhtaisia ja varoittava.

Seuraamusjärjestelmää arvioitaessa on erittäin tärkeää huomioida, että TATTI-työryhmän mietinnössä ehdotetaan kumottavaksi henkilörekisteririkosta ja henkilörekisteririkkomusta koskeva tunnusmerkistö. Käsitykseni mukaan ideana on ollut hallinnollisten sakkojen ensisijaisuus seuraamuksina (ne bis in idem). Rikosoikeudellisia seuraamuksia voitaisiin TATTI-työryhmän ehdotuksen mukaan kohdistaa vain rekisterinpitäjän tai henkilötietojen käsittelijän palveluksessa toimivaan henkilöön, joka säännösten vastaisesti käsittelee henkilötietoja (nk. urkintarikos).

Tietosuojavaltuutetun toimisto on kannattanut TATTI-työryhmässä näkemystä, jonka mukaan tietosuoja-asetuksen kansallista liikkumavaraa ei tulisi käyttää suhteessa julkisen sektorin toimijoihin.

2. Analyysi ehdotuksesta ja huomioon otettavia seikkoja

- Seuraamusjärjestelmää on tarkasteltava kokonaisuutena. Molemmat EU:n instrumentit edellyttävät, että seuraamukset ovat oikeasuhtaisia, tehokkaita ja varoittavia. Molemmat EU:n instrumentit edellyttävät, että tilanteissa**, joissa ei määrätä hallinnollisia sakkoja**, jäsenvaltiot **vahvistavat säännökset** rikkomisen vuoksi määrättäviä **seuraamuksia** varten sekä toteuttaa kaikki **tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi**.

- Toisin sanoen EU-oikeuden tehokkaan toimeenpanon näkökulmasta seuraamusjärjestelmä on pakollinen, eikä se ole tietosuoja-asetuksen puolella nk. kansallisen liikkumavaran piirissä.

- Seuraamukset kohdistetaan tapauksen mukaan rekisterinpitäjään tai/ja henkilötietojen käsittelijään, jotka vastaavat henkilötietojen käsittelyn lainmukaisuudesta (ei yksittäiseen virkamieheen/työntekijään).

- Perustuslakivaliokunta on vakiintuneesti katsonut, että lainvastaisesta teosta määrättävä maksu on rangaistusluonteinen taloudellinen seuraamus. Valiokunta on asiallisesti rinnastunut tällaiset seuraamukset rikosoikeudellisiin seuraamuksiin (mm. PeVL 61/2014, PeVL 9/2012).

- Käsitykseni mukaan uhkasakko ei ole seuraamus vaan hallinnollinen tehoste päävelvoitteen noudattamisen varmistamiseksi. Lisäksi EIT on asiassa I v. Suomi (asia 20511/03 tuomion kohta 47) todennut, ettei vahingonkorvausvastuu ole riittävä henkilötietojen suojakeino vaan alun alkaen olisi vaadittu käytännöllisiä ja tehokkaita keinoja estämään oikeudeton pääsy henkilötietoihin. Kun tällaisia ei ollut, määrättiin Suomi maksamaan vahingonkorvausta siitä, ettei se ollut kyennyt riittävällä tavalla turvaamaan yksityiselämän suojaa.

- Seuraamusjärjestelmää koskevassa kokonaisarviossa muita valvontaviranomaisen korjaavia toimivaltuuksia on kansallisen oikeusjärjestelmän valossa tarkasteltava suhteessa niiden seuraamusluonteeseen. Tarkastelu on suoritettava kokonaisvaltaisesti korjaavien toimivaltuuksien tarkoituksen ja riittävyyden (tehokas ja varoittava) näkökulmasta.

- Muut korjaavat toimivaltuudet voivat olla riittävä ja oikeasuhtainen keino korjata tietosuojasäännösten vastainen asiantila ja saattaa henkilötietojen käsittely lainmukaiseksi. Käsitykseni mukaan asiaan liittyvän EU-oikeuden mukaan hallinnolliset sakot eivät ole kaikissa tapauksissa ensisijainen keino puuttua lainvastaiseen henkilötietojen käsittelyyn vaan niiden käyttöä on arvioitava tapauskohtaisesti.

- Keskeinen ongelma suunnitellussa uhkasakko -mallissa on, että säännöksiä ja tilanteita, joiden rikkomisia ei voida tehokkaasti korjata muilla korjaavilla toimenpiteillä. Tällaisia ovat esimerkiksi henkilötietojen tietoturvaloukkaus, joka johtuu rekisterinpitäjän laiminlyönnistä, käsittely ilman käsittelyn oikeusperustetta, jo tapahtunut tietojen siirto kolmansiin maihin ilman perustetta…

- Seuraamusjärjestelmän kannalta ei ole riittävää, että rekisterinpitäjä/henkilötietojen käsittelijä itse korjaa lainvastaisen toiminnan (siinä vaiheessa, kun valvontaviranomainen puuttuu siihen) vaan tietyissä tilanteissa tietyin kriteerein lainvastaisesta toiminnasta on voitava kohdistaa toimijoihin oikeasuhtainen ja tehokas seuraamus.

- Ehdotettu sääntely johtaa siihen, vaikka asiantila korjattaisiin, tapahtuneesta säännösten rikkomisesta ei seuraisi mitään seuraamusta. Tällainen tilanne ei ole käsittääkseni mahdollinen EU:n tietosuojasäännösten valossa.

- On otettava huomioon, että esimerkiksi käsittelykieltoa ei voitaisi todennäköisesti määrätä viranomaistoiminnan yhteydessä. Esimerkiksi, jos terveydenhuollon yksikölle asetettaisiin käsittelykielto potilastietojärjestelmään, johtaisi se hyvin suurella todennäköisyydellä potilaiden terveyden vakavaan vaarantamiseen ja kuolemiin.

- Jo nyt on nähtävissä tietosuoja-asetuksen seuraamusjärjestelmän vahvistumisen (hallinnollisten sakkojen) preventiivinen vaikutus ja, miten se on vaikuttanut halukkuuteen resursoida tietosuojaan. Huomioon tulisi ottaa myös kilpailunäkökohdat, vaikka julkisen sektorin toiminta tyypillisesti painottuu lakisääteisten tehtävien hoitamiseen.

- Rekisteröidyn oikeuteen saada vahingonkorvausta laittomasta käsittelystä heikentyy olennaisesti, kun rekisterinpitäjä/henkilötietojen käsittelijä rikkomuksista ei ole enää mahdollista hakea

rekisterinpitäjältä korvausta rikosperusteisesti. Aineettomissa vahingonkorvauskanteissa on suuria vaikeuksia näyttää toteen aiheutettu vahinko, vaikka kyse olisikin ankarasta vastuusta.

- Tällä hetkellä tietosuojalautakunnalla on oikeus asettaa päätöksensä (käsittelykielto tai velvoite korjata toiminta tietynlaiseksi tietyssä määräajassa) uhkasakko. Näin ollen uhkasakosta säätäminen ei tuo mitään ”uutta” seuraamusjärjestelmään. Seuraamusjärjestelmä päinvastoin heikkenee, kun rikosoikeudellisia seuraamuksia ei voitaisi TATTI-työryhmän ehdotuksen perusteella kohdistaa rekisterinpitäjiin.

- Sen sijaan, että seuraamusjärjestelmää heikennettäisiin entisestään, jatkovalmistelussa onkin arvioitava, onko edes nykyinen järjestelmä riittävän tehokas oikeussuojakeino (joka täyttää EU-oikeudessa säädetyt reunaehdot), vaikka rikosoikeudellista seuraamusjärjestelmää kehitettäisiinkin.

- Toistuvasti julkisuudessakin esiintyy viranomaisten osalta tietovuotoja ja henkilötietojen käsittelyä, joissa on ilmeisesti rikottu henkilötietojen suojaa koskevia periaatteita ja säännöksiä. Rikosoikeudellinen seuraamus voi voimassa olevien säännösten nojalla kohdistua joko rekisterinpitäjän vastuuhenkilöön tai laittomasti henkilötietoja käsitelleeseen henkilöön. Vaikka rikos olisi tapahtunutkin rekisterinpitäjän edustajan osalta, rikosoikeudellista seuraamusta ei voida kaikissa tapauksissa määrätä, koska esimerkiksi vastuunjako viranomaisten sisällä jää epäselväksi tai riittävää näyttöä syyllisyydestä ei muutoin saada. Kaikissa tapauksissa, joissa henkilötietojen suojaa koskevia sääntöjä on todennäköisesti rikottu ei edes suoriteta esitutkintaa. Edellä mainittu johtaa siihen, että osa viranomaisten toimesta tapahtuneista säännösten rikkomisesta ei ole minkäänlaisten seuraamusten kohteena. Tällöin voidaan perustellusti esittää kysymys siitä, onko nykyinen järjestelmä tehokas, oikeasuhtainen ja varoittava?

- Lopputuloksena julkisella sektorilla virkavastuu korostuu tai jäisi ainoaksi seuraamukseksi. Julkishallinnollisen yhteisöön ei kohdistuisi rekisterinpitäjänä mitään seuraamusuhkaa. Jos tietojärjestelmä ja sen suojaus ovat kelvottomia on väärin kohdistaa moitearviointi yksittäiseen virkamieheen käyttäjänä vaan se tulisi kohdistaa viranomaiseen rekisterinpitäjänä.

- Tunnistan hallinnollisten sakkojen käyttöön liittyvät budjettitalouteen liittyvät ”ongelmat”. Tämä ei kuitenkaan voi olla esteenä tai syynä sille, miksi kansallisesti ei toimeenpanna tehokasta, oikeasuhtaista ja varoittavaa seuraamusjärjestelmää.

Yhteenvetona

1. Seuraamusjärjestelmää on tarkasteltava kokonaisuutena.

2. Seuraamusjärjestelmä on kansallisesti sitovien EU-velvoitteiden nojalla pakollinen.

3. Kyse ei ole ainoastaan siitä, voidaanko viranomaisille määrätä hallinnollisia sakkoja vaan kokonaisuudessa seuraamusjärjestelmän olemassa olosta ja tietosuojasääntelyn tehokkaasta toimeenpanosta siten kuin EU-oikeus siihen jäsenvaltioita velvoittaa. Jos

kansallisesti päädytään siihen, ettei viranomaisille voida määrätä hallinnollisia sakkoja (ml. tiettyyn euromäärään alennetut sakot), on lainsäätäjän tehtävänä varmistua tehokkaan, varoittavan ja oikeasuhtaisen seuraamusjärjestelmän olomassa olosta ja sen täytäntöönpanosta.

4. Tilanne, jossa seuraamus kohdistuu vain laiminlyönnin korjaamiseen, ei vastaa direktiivissä ja asetuksessa säädettyjä edellä esitettyjä reunaehtoja seuraamusjärjestelmälle, koska muutoin lainvastainen henkilötietojen käsittely jäisi ainakin tietyiltä osin kokonaan pakollisen seuraamusjärjestelmän ulkopuolelle.

Postiosoite	**Käyntiosoite**	**Vaihde**	**Sähköposti ja kotisivut**
PL 800	Ratapihantie 9	029 56 66700	tietosuoja@om.fi
00521 Helsinki	6. kerros		http://www.tietosuoja.fi
Neuvonta	029 56 16670	ma-to 9:00–11:00 & 13:00–15:00 pe 9:00–12:00	