

Asia: VN/24616/2022

Lausuntopyyntö arviomuistiosta poliittisesti vaikutusvaltaisten henkilöiden henkilötietojen käsittelystä keskitetyn kansallisen tietojärjestelmän avulla

Kysymykset vastaanottajille

1. Kuinka tarpeellisena näette poliittisesti vaikutusvaltaisten henkilöiden tai tällaisten henkilöiden perheenjäsenten tai yhtiökumppanien henkilötietojen käsittelyn keskitetyn kansallisen tietojärjestelmän avulla?

Poliisihallitus kannattaa keskitetyn tietojärjestelmän perustamista kansallisesti PEP-henkilöistä ja heidän perheenjäsenistään ja yhtiökumppaneistaan. Keskitetty tietojärjestelmä asianmukaisesti toteutettuna parantaisi rekisteröityjen oikeuksia ja vähentäisi ilmoitusvelvollisten hallinnollista taakkaa. Keskitetyn järjestelmän rekisterinpitäjäksi tulisi säätää viranomainen, sillä viranomaisella on parhaat mahdollisuudet huolehtia tietojen ajantasaisuudesta ja luotettavuudesta, tietoturvasta ja kyberturvallisuudesta. Tarkempia huomioita toteutettavan järjestelmän osalta esimerkiksi tietosuojaan ja teknisiin ratkaisuihin on mahdollista antaa jatkovalmistelussa. Yleisesti voidaan todeta, että esitys on hyvin laadittu ja edellä mainittuja seikkoja asianmukaisesti arvioitu arviomuistiossa.

Yleisessä tietosuoja-asetuksessa huomioidaan lasten erityinen henkilötietojen suojaamisen tarve, joka onkin nostettu esiin arviomuistiossa. Rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018, rikosasioiden tietosuoja-laki) 8 §:ssä säädetään eräiden henkilötietojen erottamisesta toisistaan. Rikosasioiden tietosuojalain 8 §:n 1 momentin mukaan rekisterinpitäjän on erotettava tarvittaessa ja mahdollisuuksien mukaan selvästi toisistaan henkilötiedot, jotka koskevat käsiteltävän asian kannalta eri asemassa olevia rekisteröityjä. Lisäksi edellä mainitun pykälän 2 momentin mukaan tosiseikkoihin perustuvien henkilötietojen erottamiseksi henkilökohtaisiin arvioihin perustuvista henkilötiedoista on toteutettava kaikki kohtuulliset toimenpiteet. Poliisihallitus esittää arvioitavaksi, olisiko edellä mainittu sääntelytapa käyttökelpoinen myös perustettavassa järjestelmässä, vaikkakaan kyseiseen käsittelyyn ei sovelleta rikosasioiden tietosuojalakeja. Tällaisten henkilötietojen erottamisen voisi ajatella toimivan lisäsuojatoimina esimerkiksi lasten henkilötietojen käsittelyn ja muiden lasten oikeuksien näkökulmasta ja toisaalta tarvittaessa erottamassa virallisen tiedon ei-virallisesta.

Arviomuistion valmistelun aikana on arvioitu, että rekisteröidyn pääsy keskitettyyn kansalliseen PEP-tietojärjestelmään talletettuihin tietoihinsa olisi mahdollista toteuttaa sähköisen asiointipalvelun kautta. Tämä mahdollistaisi rekisteröidylle omien tietojen tarkastamisen, mikä lisäisi osaltaan tietojärjestelmään tallennettujen tietojen luotettavuutta. Rekisteröity pystyisi myös valvomaan sitä, mihin hänen henkilötietojaan on luovutettu, millä voitaisiin vähentää henkilötietojen suojaan liittyviä riskejä. Tämä lähtökohta on Poliisihallituksen näkemyksen mukaan sinänsä kannatettava.

Arviomuistiossa todetaan, että tietosuojasetuksen 15 artiklan mukaista rekisteröidyn oikeutta saada tieto itseään koskevien henkilötietojen käsittelystä voidaan rajoittaa tietosuojalain (1050/2018) 34 §:n nojalla. Keskitetyn kansallisen PEP-tietojärjestelmän kohdalla kyseeseen voisi lähinnä tulla tietosuojalain 34 §:n 1 momentin 1 kohta, jonka mukaan rekisteröidyllä ei ole tietosuojasetuksen 15 artiklassa tarkoitettua oikeutta tutustua hänestä kerättyihin tietoihin, jos tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta taikka haitata rikosten ehkäisemistä tai selvittämistä. Käytännössä tämä tarkoittaisi sitä, ettei rekisteröidylle annettaisi tietoa siitä, että hänen tietojaan on luovutettu rekisteristä esitutkintaviranomaisille vireillä olevan esitutkinnan vuoksi.

Poliisihallitus pitää edellä mainittua rajausta välttämättömänä huomioiden esitutkintaviranomaisten tiedon laatu ja tiedon paljastumisen haitta suojattavalle edulle. Edellä mainittu rajoitusmahdollisuus tulisi huomioida myös teknisesti, mikäli päädytään toteuttamaan rekisteröidylle oikeus tarkastaa omia tietojaan sähköisen asiointipalvelun kautta. Toteutuksen yhteydessä tulisi huomioida se, että pelkästään se, että tarkastusoikeutta on rajoitettu, voi vahingoittaa edellä mainittuja yleisiä etuja. Poliisin osalta tarkastusoikeuden toteuttamista ja rajoittamista koskevia menettelysääntöjä on henkilötietojen käsittelystä poliisitoimissa annetussa laissa (616/2019, poliisin henkilötietolaki). Tarkastusoikeuden toteuttamista koskevat menettelytavat on säädetty poliisin henkilötietolain 41 §:ssä. Poliisin henkilötietolain 42 § säädetään poikkeuksista tarkastusoikeuteen. Pykälässä yksilöityjen tietojen osalta rekisteröidyllä on tarkastusoikeus ainoastaan tietosuojavaltuutetun välityksellä.

2. Tulisiko vielä jokin näkökulma erityisesti ottaa huomioon vaikutusten arvioinnissa?

Poliisihallitus pitää hyvänä arviomuistiossa esitettyä huomiota siitä, että yleisen tietosuojasetuksen 35 artiklan mukainen tietosuojan vaikutustenarviointi toteutettaisiin jo lainsäädäntöhankkeen yhteydessä. Kun kattava vaikutustenarviointi toteutettaisiin jo lainsäädäntötyön yhteydessä, tämä voisi nopeuttaa keskitetyn järjestelmän käyttöönottoa ja vapauttaa rekisterinpitäjän tekemästä vaikutustenarviointia tai vaikutustenarviointia voitaisiin tarvittaessa täydentää vain tarvittavin osin. Tällainen vaikutustenarviointi myös vähentäisi rekisterinpitäjän hallinnollista taakkaa sekä mahdollisesti helpottaisi palvelua hyödyntävien sekä sinne tietoa tuottavien tahojen osalta palvelun käyttöönottoa.

Poliisihallitus pitää hyvänä myös arviomuistiossakin esitetystä, että jatkovalmistelussa toimialasta vastaavan ministeriön toimesta toteutettaisiin tiedonhallintalain 8 §:n 2 momentin mukainen arvio vaikutuksista tiedonhallintaan.

Kerättäessä PEP-henkilöiden ja heidän perheenjäsentensä tietoja keskitettyyn järjestelmään, voidaan erilaisten kyberhyökkäysyritysten arvioida kohdistuvan kyseiseen järjestelmään. Poliisihallituksen näkemyksen mukaan jatkovalmistelussa olisi siten hyvä arvioida mahdollisia vaikutuksia kansalliseen turvallisuuteen, ennakkollisesti varautua mahdollisiin hyökkäyksiin ja jo ennakkoon toteuttaa riittävät toimenpiteet tietojärjestelmän tekniseen ja muuhun turvallisuuteen.

3. Muuta lausuttavaa

Yleisesti voidaan todeta, että rahanpesun ja terrorismin rahoittamisen torjumiseksi on hyvä selvittää voimassaolevan lainsäädännön kattavuutta, tehokkuutta ja valmistella tarvittavat muutokset lainsäädäntöön. Poliisihallitus pitää tärkeänä, että jatkovalmistelussa turvataan riittävät tiedonsaantioikeudet poliisille samoin kuin oikeus luovuttaa tietoja rekisteriin ja että tietojen luovutusta koskeva sääntely yhteensovitetaan.

Arviomuistiossa on todettu, ettei oikeusjärjestelmä tunne hallinnollisten seuraamusten määräämistä viranomaisille. Yleistä tietosuojaa-asetusta täydentävän tietosuojalain valmistelun yhteydessä käytiin keskustelua siitä, voitaisiinko myös viranomaiselle määrätä voimassa olevan lain 24 §:ssä mainittu hallinnollinen seuraamusmaksu. Oikeusministeriö on 5.12.2023 asettanut Hallinnollisten seuraamusmaksujen määrääminen tietosuojalainsäädännön rikkomuksista julkissektorilla -nimisen hankkeen (OM127:00/2023), jonka tavoitteena on arvioida, voitaisiinko ja millä edellytyksillä tietosuojalain säännöksiä voitaisiin muuttaa siten, että lain rikkomisesta voidaan määrätä hallinnollisia seuraamusmaksuja myös viranomaisille. Jatkovalmistelua varten voi siten olla merkitystä sillä, että oikeuskäytäntö voi olla muuttumassa tai ainakin tällaista vaihtoehtoa selvitetään.

Arviomuistiossa todetaan, että perustuslakivaliokunnan mukaan hallinnollisen seuraamuksen yleisistä perusteista on säädettävä perustuslain 2 §:n 3 momentin edellyttämällä tavalla lailla, koska sen määräämiseen sisältyy julkisen vallan käyttöä. Muistioon kirjatun mukaan valiokunta on lisäksi katsonut, että myös uhkasakon määräämisen osalta kyse on merkittävästä julkisen vallan käytöstä.

Esimerkiksi työsuojelun valvontaa suorittavat viranomaiset voivat määrätä valvonnan kohteella oleville julkishallinnon organisaatioille uhkasakkoja epäkohtien korjaamiseksi. Myös tietosuojalaissa ja rikosasioiden tietosuojalaissa on tietosuojavaltuutetulle eräissä tilanteissa mahdollistettu uhkasakon määrääminen. Poliisihallituksen näkemyksen mukaan keskeistä on huolehtia siitä, että rekisterin avaamisen yhteydessä tietoja ilmoittaville organisaatioille on tarjota riittävää tukea järjestelmän käytön ja käyttöprosessin tukemiseksi esimerkiksi perustamalla sivusto, josta on saatavilla koulutusta, ohjeita rekisteröintiin ja muuta tukimateriaalia.

Muistiossa on myös esitetty, että väärän tiedon antaminen rekisterissä tulisi selvittää rikosprosessissa ja epäilty rikos olisi rekisterimerkintärikos (RL 16:8) tai väärän todistuksen antaminen viranomaiselle (RL 16:8). Kuten muistiossakin on todettu, niin rekisterimerkintärikoksen ja väärän todistuksen antaminen viranomaiselle tunnusmerkistön täytyminen edellyttää tekijältään tahallisuutta. Jälkimmäisen rikoksen osalta hallituksen esityksessä (HE 6/1997) on todettu, että

"Todistuksen sisällön tulee olla tekijän tietien totuudenvastainen. Tahallisuuteen ei riitä tietoisuus, että todistus mahdollisesti on väärä". Muistiossa on käyty läpi poliittisesti vaikutusvaltaisen henkilön sekä tämän läheisten määrittelyn haastavuutta ja kun tunnistaminen jatkossakin perustuisi pitkälti ao. henkilön omaan ilmoitukseen on todennäköistä, että tahallisuuden osoittaminen on käytännössä hyvin vaikeaa. On myös huomattava, että poliittisesti vaikutusvaltaiset henkilöt voivat olla ulkomaan kansalaisia, jolloin erehtymisen mahdollisuus ilmoitusvelvollisuuteen ja tietojen antamiseen liittyen voi olla suurempi kuin Suomen kansalaisilla.

Esitetyn rikosprosessin osalta olisi selvitettävä mahdollisuutta sille, että seuraamusharkinnasta ja seuraamuksista vastaisi rekisterin tietosisällöstä vastaava ja valvontaa suorittava viranomainen sen sijaan, että asia vietäisiin rikosprosessiin, jonka todennäköinen seuraamus virheelliseksi todetun rekisterimerkinnän osalta olisi sakkorangaistus, ellei esitutkinnassa tai myöhemmässä vaiheessa todettaisi kyseessä olevan korkeintaan tuottamus tai erehdys. Rikosprosessin sijaan tulisi varmistaa, että ilmoitusvelvollisuuden valvontaa suorittavalla viranomaisella on riittävät resurssit ja mahdollisuudet neuvoa, ohjata ja mahdollisesti tarvittaessa sanktioiden kautta puuttua siihen, että rekisteriin merkittävät tiedot ovat oikeita. Vaikka kyse on viranomaisen ylläpitämästä rekisteristä, tulisi selvittää mahdollisuutta sille, että edellä mainituilla keinoilla voidaan varmistaa rekisterin tietosisällön pysyminen oikeana ja viimesijaisena keinona olisi asian vieminen rikosprosessiin. Kysymys on myös viranomaisten resurssien tehokkaasta käytöstä ja valvontaa suorittavalla viranomaisella olisi tässä tapauksessa parempi käsitys valvonnan kohteesta ja toiminnan tahallisuudesta.

Mikäli lainvalmistelussa päädytään siihen, että asia tulisi käsitellä rikosprosessissa, vaikutukset poliisin resursseihin tulee jatkovalmistelussa erikseen arvioida. Lisäksi tiedonsaantia koskevan sääntelyn osalta on erityisesti säädettävä siitä, että poliisilla on rikosten estämistä, paljastamista ja selvittämistä varten oltava oikeus saada tietoja rekisteristä. Rahanpesun selvittelykeskukselle lakiin kirjattu tiedonsaantioikeus koskee nimenomaan rahanpesun ja terrorismin rahoituksen torjuntaa ja ei sellaisenaan kattaisi riittävällä tavalla poliisin tiedonsaantioikeuksia. Poliisihallitus pyytää tässä yhteydessä huomioimaan myös Keskusrikospoliisin lausunnossa esitetyn.

Poliisihallitus siten yhtyy arviomuistiossa esitettyyn näkemykseen siitä, että keskitetyn kansallisen PEP-tietojärjestelmän rekisterinpitäjän mahdollisia sanktiovaltuuksia ja hallinnollisia seuraamuksia tulisi tarkastella yksityiskohtaisemmin jatkovalmistelussa.

Nieminen Jaana
Poliisihallitus