Hallituksen esitys eduskunnalle laiksi Euroopan unionin tietojärjestelmien yhteentoimivuudesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki Euroopan unionin tietojärjestelmien yhteentoimivuudesta. Laissa annettaisiin kehyksen vahvistamisesta poliisiyhteistyötä ja oikeudellista yhteistyötä sekä turvapaikka- ja muuttoliikeasioita koskevien EU:n tietojärjestelmien yhteentoimivuudesta ja kehyksen vahvistamisesta rajoja ja viisumipolitiikkaa koskevien EU:n tietojärjestelmien yhteentoimivuudesta annettuja Euroopan unionin asetuksia täydentävät säännökset toimivaltaisista viranomaisista ja pääsystä yhteiseen henkilöllisyystietovarantoon.

Ehdotettu laki on tarkoitettu tulemaan voimaan 1. päivänä syyskuuta 2022

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Esityksen valmisteluun ovat johtaneet 9. kesäkuuta 2019 voimaan tulleet Euroopan parlamentin ja neuvoston asetus (EU) 2019/818 kehyksen vahvistamisesta poliisiyhteistyötä ja oikeudellista yhteistyötä sekä turvapaikka- ja muuttoliikeasioita koskevien EU:n tietojärjestelmien yhteentoimivuudelle (engl. Interoperability) ja asetusten (EU) 2018/1726, (EU) 2018/1862 ja (EU) 2019/816 muuttamisesta (jäljempänä *poliisiyhteentoimivuusasetus)* ja Euroopan parlamentin ja neuvoston asetus (EU) 2019/817, kehyksen vahvistamisesta rajoja ja viisumipolitiikkaa koskevien EU:n tietojärjestelmien yhteentoimivuudelle ja Euroopan parlamentin ja neuvoston asetusten (EY) N:o 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 ja (EU) 2018/1861 sekä neuvoston päätösten 2004/512/EY ja 2008/633/YOS muuttamisesta (jäljempänä *rajayhteentoimivuusasetus.*

Asetusehdotusten antamisen taustalla oli muuttoliikekriisiin liittynyt luvattomien rajanylitysten lisääntyminen sekä terrori-iskut. Euroopan komissio (jäljempänä *komissio*) katsoi, että EU:n sisäisen turvallisuuden vahvistamiseksi tiedonhallinnan tuloksellisuutta ja tehokkuutta tulee lisätä perusoikeuksia ja erityisesti henkilötietojen suojaa kunnioittaen. Näin voidaan suojata paremmin EU:n ulkorajoja, parantaa muuttoliikkeen hallintaa ja lisätä sisäistä turvallisuutta kansalaisten edun mukaisesti.

EU:n tasolla on jo käytössä ja kehitteillä useita tietojärjestelmiä, joiden avulla rajavartijat sekä maahanmuutto- ja lainvalvontaviranomaiset rekisteröivät ja saavat käyttöönsä henkilöitä koskevia tietoja. Käytössä olevia tietojärjestelmiä ovat EU:n viisumitietojärjestelmä (VIS), turvapaikanhakijoiden sormenjälkitietojärjestelmä (Eurodac) ja Schengenin tietojärjestelmä (SIS) sekä uusina järjestelminä rakennetaan rajanylitystietojärjestelmä (EES), Euroopan matkustustieto- ja -lupajärjestelmä (ETIAS) sekä keskitetty järjestelmä niiden jäsenvaltioiden tunnistamiseksi, joilla on kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tuomioita koskevia tietoja (ECRIS-TCN). Järjestelmät ovat toisiaan täydentäviä ja, lukuun ottamatta SIS:ä, ne koskevat ainoastaan kolmansien maiden kansalaisia. Henkilötietojen määrällä tarkasteltuna suurimpia järjestelmiä ovat EES, ETIAS ja VIS, jotka koskevat vain kolmansien maiden kansalaisia. Jotta EU:n tietojärjestelmien tarjoama tuki olisi tuloksellista, niistä saatavien tietojen on oltava kattavia, tarkkoja ja luotettavia. Komission mukaan EU:n tietoarkkitehtuurissa on kuitenkin rakenteellisia puutteita. Kansallisilla viranomaisilla on käytössään eri tavoin hallinnoiduista tietojärjestelmistä muodostuva monimutkainen kokonaisuus. Lisäksi rajaturvallisuutta ja sisäistä turvallisuutta koskeva tietoarkkitehtuuri on hajanainen, sillä tiedot tallennetaan erikseen eri järjestelmiin, joita ei ole kytketty toisiinsa. Tämä johtaa katvealueisiin, joka muun muassa helpottaa väärien henkilötietojen käyttöä. Seurauksena on, että EU:n tason tietojärjestelmät eivät ole tällä hetkellä yhteentoimivia eli sellaisia, että niiden avulla olisi mahdollista vaihtaa ja jakaa tietoja niin, että viranomaiset ja toimivaltaiset virkamiehet saisivat tarvitsemansa tiedot, milloin ja missä niitä tarvitaankin.

Myös Euroopan parlamentti oli kiirehtinyt toimenpiteitä, joilla parannetaan ja kehitetään olemassa olevia tietojärjestelmiä, pureudutaan ongelmiin, jotka edesauttavat tietokatkoja ja pyritään kohti EU-tason tietojärjestelmien yhteentoimivuutta sekä tehokkaampaa tietojenvaihtoa EU-tasolla.

1.2 Valmistelu

EU-säädöksen valmistelu

Komissio antoi 12.12.2017 ehdotukset poliisiyhteentoimivuusasetukseksi (COM(2017) 794 final) ja rajayhteentoimivuusasetukseksi (COM(2017) 793 final). Asetusten yleinen tavoite on parantaa Schengenin ulkorajojen hallintaa sekä unionin sisäistä turvallisuutta. Asetukset jouduttiin antamaan erillisinä, koska jäsenmaiden osallistumisessa on eroja politiikka-alueiden välillä ja ehdotusten oikeusperustat poikkeavat toisistaan.

Neuvottelujen jälkeen Euroopan parlamentti ja neuvosto hyväksyivät asetukset ja ne tulivat voimaan 9.6.2019. Asetusten täysimääräinen soveltaminen aloitetaan komission päättämänä ajankohtana.

Valtioneuvosto on informoinut eduskuntaa yhteentoimivuutta koskevista EU-asetusehdotuksista U-kirjelmällä U 7/2018 vp, josta hallintovaliokunta (HaVL6 2018 vp) ja perustuslakivaliokunta (PeVL11 2018 vp) antoivat lausuntonsa. Kokonaisuuteen liittyvät myös kutakin EU:n laajuista tietojärjestelmää (EES, ETIAS, SIS, VIS, Eurodac, ECRIS-TCN) tai niiden muuttamista koskevat asetusehdotukset.

Yhteentoimivuuteen liittyvät tietojärjestelmätoiminnallisuudet rakennetaan vaiheittain vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston (eu-LISA) toimesta vuoteen 2024 mennessä. Yhteentoimivuus ja tiedon eheys edellyttävät Euroopan laajuista yhteistyötä sekä yhtäaikaista toteutusta ja käyttöönottoa.

Hallituksen esityksen valmistelu

Hallituksen esityksen valmistelua varten perustettiin työryhmä 2.4.2020. Työryhmässä olivat edustettuina sisäministeriön poliisiosasto, rajavartio-osasto, hallinto- ja kehittämisosasto ja maahanmuutto-osasto, valtiovarainministeriö, oikeusministeriö, ulkoasiainministeriö, Poliisihallitus, suojelupoliisi, keskusrikospoliisi, Tulli ja Maahanmuuttovirasto.

Hallituksen esityksen tausta-aineisto on saatavilla osoitteessa Lainsäädäntöhanke kehyksen vahvistamisesta EU:n tietojärjestelmien yhteentoimivuudelle - Sisäministeriö (intermin.fi) hankenumerolla SM008:00/2020.

2 EU-säädösten tavoitteet ja pääasiallinen sisältö

Poliisi- ja rajayhteentoimivuusasetusten tavoitteena on erityisesti:

1. Varmistaa, että loppukäyttäjillä on nopea, saumaton, systemaattinen ja kontrolloitu pääsy tietoon, jota ne tarvitsevat tehtäviensä hoitamisessa.

2. Antaa ratkaisu, jolla paljastetaan samoihin biometrisiin tietoihin liitetyt eri henkilöllisyydet. Tämä mahdollistaa väärän henkilöllisyyden käyttämisen torjunnan.

3. Helpottaa kolmannen maan kansalaisten henkilöllisyyden tarkistamista.

4. Nopeuttaa ja virtaviivaistaa lainvalvontaviranomaisten pääsyä muihin kuin lainvalvontatarkoitusta varten perustettuihin järjestelmiin, jos pääsy on tarpeellinen vakavan rikollisuuden ja terrorismin ennalta estämiseksi, paljastamiseksi ja teoista syyttämiseksi.

Asetukset ovat suoraan sovellettavia. Asetusten johdosta kansallista sääntelyä tulee muuttaa siltä osin, kuin asetukset edellyttävät kansallisen lainsäädännön antamista tai kansallinen, voimassa oleva lainsäädäntö on ristiriidassa asetusten kanssa.

2.1 Poliisiyhteentoimivuusasetus

2.1.1 Yleiset säädökset

Asetuksen I luvussa käsitellään yleisiä säädöksiä. Poliisiyhteentoimivuusasetuksella yhdessä Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/817 (28) kanssa vahvistetaan kehys, jolla varmistetaan yhteentoimivuus rajanylitystietojärjestelmän (EES), viisumitietojärjestelmän (VIS), Euroopan matkustustieto- ja -lupajärjestelmän (ETIAS), Eurodacin, Schengenin tietojärjestelmän (SIS) ja keskitetty järjestelmä niiden jäsenvaltioiden tunnistamiseksi, joilla on kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tuomioita koskevia tietoja (ECRIS-TCN) välillä.

Kehys sisältää seuraavat yhteentoimivuuskomponentit:

a. Eurooppalainen hakuportaali (ESP), jonka kautta voidaan tehdä samanaikaisia hakuja useissa tietojärjestelmissä.

b. Yhteinen biometrinen tunnistuspalvelu (yhteinen BMS).

c. Yhteinen henkilöllisyystietovaranto (CIR).

d. Rinnakkaishenkilöllisyyksien tunnistin (MID).

Lisäksi asetuksessa säädetään tietojen laatuvaatimuksista, UMF-viestimuodosta (universal message format) ja raportoinnin ja tilastoinnin keskustietoarkistosta (CRRS) sekä jäsenvaltioiden ja vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston (eu-LISA) vastuualueista yhteentoimivuuskomponenttien suunnittelussa, kehittämisessä ja toiminnassa.

Luvussa säädetään myös asetuksessa käytettävistä määritelmistä. Asetuksen 4 artiklan 19 kohdassa on määritelty poliisiviranomainen. Määritelmässä viitataan poliisiviranomaisten osalta Euroopan parlamentin ja neuvoston direktiiviin (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta ja sen 3 artiklan 7 alakohdassa määriteltyyn toimivaltaiseen viranomaiseen. Määritelmän mukaan toimivaltaisella viranomaisella tarkoitetaan a) kaikkia viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvät syytetoimet tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy; tai b) kaikkia muita elimiä tai yksiköitä, joille on jäsenvaltion lainsäädännössä annettu tehtäväksi käyttää julkista valtaa tai valtuuksia rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syytetoimiin tai rikosoikeudellisten seuraamusten

täytäntöönpanoon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy.

Asetusta sovelletaan Eurodac-, SIS- ja ECRIS-TCN-järjestelmiin. Lisäksi asetusta sovelletaan myös Europolin tietoihin siltä osin, että niistä on mahdollista tehdä kyselyjä samanaikaisesti kuin edellä mainituista EU:n tietojärjestelmistä. Asetuksen soveltamisala on 3 artiklassa rajattu henkilöihin, joiden osalta henkilötietoja voidaan käsitellä artiklassa tarkoitetuissa EU:n tietojärjestelmissä ja Europolin tiedoissa.

2.1.2 Yhteentoimivuuskomponentit

Asetuksen II luvussa säädetään eurooppalaisesta hakuportaalista (ESP), III luvussa yhteisestä biometrisestä tunnistuspalvelusta (BMS), IV luvussa yhteisestä henkilöllisyystietovarannosta (CIR) ja V luvussa rinnakkaishenkilöllisyyksien tunnistimesta (MID).

Asetuksella perustetaan ESP, jolla helpotetaan jäsenvaltioiden viranomaisten ja unionin virastojen nopeaa, saumatonta, tehokasta, järjestelmällistä ja valvottua pääsyä niiden käyttöoikeuksien puitteissa EU:n tietojärjestelmiin, Europolin tietoihin ja Interpolin tietokantoihin niiden tehtävien suorittamiseksi sekä jolla tuetaan EES-, VIS-, ETIAS-, Eurodac-, SIS- ja ECRIS-TCN-järjestelmien tavoitteita ja tarkoituksia. ESP:llä ei tarkoiteta loppukäyttäjälle näkyvää sivustoa vaan se on toiminto, jonka kautta kansallisten käyttöliittymien avulla syötetyt haut toteutetaan yhteentoimivuuskehyksessä.

Asetuksella perustetaan BMS, jonne tallennetaan CIR:iin ja SIS-järjestelmään tallennetuista tiedoista saatuja biometrisiä malleja. Näin mahdollistetaan kyselyjen tekemisen biometrisillä tiedoilla useista EU:n tietojärjestelmistä, sekä CIR:n ja MID:n toiminta sekä EES-, VIS-, Eurodac, SIS- ja ECRIS- TCN-järjestelmien tavoitteiden tukeminen.

Asetuksella perustetaan myös yhteinen henkilöllisyystietovaranto (CIR), johon luodaan kustakin EES-, VIS-, ETIAS-, Eurodac- tai ECRIS-TCN-järjestelmään rekisteröidystä henkilöstä yksilökohtainen tiedosto, jotta voidaan helpottaa ja tukea EES-, VIS-, ETIAS-, Eurodac- ja ECRIS-TCN-järjestelmiin rekisteröityjen henkilöiden virheetöntä tunnistamista, tukea MID:n toimintaa sekä helpottaa ja virtaviivaistaa nimettyjen viranomaisten ja Europolin pääsyä EES-, VIS-, ETIAS- ja Eurodac-järjestelmiin, jos se on tarpeen terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi asetuksen 22 artiklan mukaisesti.

Artiklassa 18 säädetään niistä tiedoista, jotka tallennetaan CIR:iin. Artiklassa viitataan asetukseen EU 2019/816 niiden jäsenvaltioiden tunnistamista koskevan keskitetyn järjestelmän perustamisesta, joilla on kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tuomioita koskevia tietoja (ECRIS-TCN), eurooppalaisen rikosrekisteritietojärjestelmän täydentämiseksi ja asetuksen (EU) 2018/1726 muuttamisesta. Artiklan 18 mukaisesti tallennettavia tietoja ovat tiedot, jotka pidetään loogisesti erotettuina sen tietojärjestelmän mukaan, josta tiedot ovat peräisin, eli asetuksen (EU) 2019/816 5 artiklan 1 kohdan b alakohdassa ja 2 kohdassa tarkoitetut tiedot, joita ovat b) sormenjälkitietojen osalta: i) sormenjälkitiedot, jotka on otettu kansallisen lainsäädännön mukaisesti rikosasian käsittelyn yhteydessä; ii) vähintään jommankumman seuraavan perusteen nojalla otetut sormenjälkitiedot: kun kolmannen maan kansalainen on tuomittu vähintään kuuden kuukauden vankeusrangaistukseen; tai kun kolmannen maan kansalainen on tuomittu rikoksesta, josta voidaan määrätä jäsenvaltion lainsäädännön mukaisesti enimmillään vähintään 12 kuukauden vankeusrangaistus.

Asetuksen 20 artiklassa säädetään pääsystä CIR:iin henkilön tunnistamista varten. Sen 1 kohdan mukaan poliisiviranomainen tekee kyselyjä CIR:stä 2 ja 5 kohdan mukaisesti ainoastaan

seuraavissa olosuhteissa: a) poliisiviranomainen ei kykene tunnistamaan henkilöä matkustusasiakirjan tai kyseisen henkilön henkilöllisyyden todistavan muun uskottavan asiakirjan puuttumisen vuoksi; b) henkilön antamista henkilöllisyystiedoista on epäilyjä; c) henkilön antaman matkustusasiakirjan tai muun uskottavan asiakirjan aitoudesta on epäilyjä; d) matkustusasiakirjan tai muun uskottavan asiakirjan haltijan henkilöllisyydestä on epäilyjä; tai e) henkilö ei kykene yhteistyöhön tai kieltäytyy siitä. Artiklan mukaan tällaisia kyselyjä ei saa tehdä alle 12-vuotiaista alaikäisistä, paitsi jos se on lapsen edun mukaista.

Artiklan 20 kohdan 2 mukaan, kun kyse on joistakin edellä mainituista olosuhteista, poliisiviranomainen, jolle on annettu kansallisella säädöksellä tähän valtuudet, saa yksinomaan henkilön tunnistamiseksi tehdä kyselyjä CIR:stä kyseisen henkilön biometrisillä tiedoilla, jotka on saatu paikalla henkilöllisyyden selvittämisen yhteydessä, edellyttäen, että menettely on käynnistetty kyseisen henkilön läsnä ollessa. Jos kysely osoittaa, että CIR:ään on tallennettu kyseistä henkilöä koskevia tietoja, poliisiviranomaisella on pääsy katsomaan 18 artiklan 1 kohdassa tarkoitettuja tietoja. Jos henkilön biometrisiä tietoja ei voida käyttää tai jos kysely kyseisillä tiedoilla epäonnistuu, kysely tehdään kyseisen henkilön henkilöllisyystiedoilla yhdessä matkustusasiakirjan tietojen kanssa tai kyseisen henkilön antamilla henkilöllisyystiedoilla. Lisäksi poliisiviranomainen, jolle on annettu kansallisella säädöksellä tähän valtuudet, saa luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa ja yksinomaan sellaisten tuntemattomien henkilöiden tunnistamiseksi, jotka eivät pysty osoittamaan henkilöllisyyttään, tai tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi tehdä kyselyjä CIR:stä kyseisten henkilöiden biometrisillä tiedoilla.

Artiklan 20 kohdat 5 ja 6 velvoittavat jäsenvaltiot, jotka haluavat käyttää artiklassa toimivaltaisille viranomaisille säädettyjä mahdollisuuksia päästä yhteiseen henkilöllisyystietovarantoon, antamaan tästä kansallisia säädöksiä. Artiklan 5 kohdan mukaan jäsenvaltioiden, jotka haluavat käyttää säädettyä mahdollisuutta, on annettava tästä kansallinen säädös. Jäsenvaltioiden on tällöin otettava huomioon tarve välttää kolmansien maiden kansalaisiin kohdistuva syrjintä. Lisäksi todetaan, että tällaisessa säädöksessä on täsmennettävä tunnistamiselle täsmällinen artiklassa todettu tarkoitus. Jäsenvaltioiden on nimettävä toimivaltaiset poliisiviranomaiset ja vahvistettava henkilöllisyyden selvittämisen menettelyt, edellytykset ja kriteerit.

Artiklassa 21 säädetään pääsystä CIR:iin henkilöllisyyksien tunnistamista varten.

Artiklassa 22 säädetään niistä CIR:iin tehtävistä kyselyistä, joiden tarkoituksena on vakavien terrorismirikosten tai muiden vakavien rikosten torjuminen, havaitseminen tai tutkinta. Kohdan 1 mukaan nimetyt viranomaiset ja Europol voivat hakea CIR:istä tiedon, onko Eurodacissa tietoja tietystä henkilöstä. Tällainen haku on sallittua tehdä yksittäistapauksessa, kun on perusteltu syy uskoa, että haku edistää terrorismi- tai muiden vakavien rikosten torjumista, havaitsemista tai tutkimista. Erityisesti näin voidaan toimia, jos epäillään että terrorismi- tai muusta vakavasta rikoksesta epäillyn tai tällaisen rikoksen uhrin tiedot on tallennettu Eurodaciin.

Kohdassa 2 säädetään CIR:in ilmoittamasta Eurodac-vastaavuuden muodosta. CIR antaa Europolille ja nimetyille viranomaisille artiklan 18 kohdan 2 mukaisen vastauksen, jossa ilmoitetaan Eurodacin sisältävän kyselyä vastaavaa tietoa. Kun vastaavuus on todettu, esittää Europol tai nimetty viranomainen pyynnön rajoittamattomasta pääsystä vähintään yhteen tietojärjestelmään niistä, joista vastaavuus on löytynyt. Mikäli pyyntöä rajoittamattomasta pääsystä ei poikkeuksellisesti tehdä, on nimettyjen viranomaisten kirjattava perustelut tekemättä jättämiselle. Perustelujen tulee olla johdettavissa kansalliseen tiedostoon. Europol vastaa perustelujen kirjaamisesta asiaa koskevaan tiedostoon.

Viidennessä luvussa säädetään MID:stä. Tarkoituksena on tunnistaa rinnakkaishenkilöllisyyksiä ja torjua henkilöllisyyspetoksia sekä tukea CIR:n, EES:n, VIS:n, ETIAS:n, Eurodacin, SIS:n ja ECRIS-TNC:n tavoitteita.

Luvut sisältävät myös säädökset tietojen säilyttämisestä ja lokitietojen eli tietojenkäsittelytoimien säilyttämisestä.

2.1.3 EU:n tietojärjestelmissä olevien tietojen väliset linkit

MID:in tavoitteena on luoda linkkejä EU:n eri tietojärjestelmissä olevien tietojen välille ja tallentaa ne rinnakkaishenkilöllisyyksien havaitsemiseksi. Tällä pyrittäisiin sekä helpottamaan vilpittömässä mielessä matkustavien henkilöllisyyden selvittämistä että torjumaan henkilöllisyyspetoksia.

Artiklassa 30 säädetään keltaisesta linkistä. Jos rinnakkaishenkilöllisyyksien manuaalista todentamista ei ole vielä tehty, tietojen välinen linkki luokitellaan keltaiseksi silloin, kun linkitetyillä tiedoilla a) on samat biometriset tiedot, mutta erilaiset tai samankaltaiset henkilöllisyystiedot, b) henkilötiedot ovat eri, mutta matkustusasiakirjan tiedot ovat samat, eikä henkilön biometrisiä tietoja ole tallennettu mihinkään EU:n tietojärjestelmään, c) henkilöllisyystiedot ovat samat, mutta biometriset tiedot poikkeavat toisistaan sekä d) henkilöllisyystiedot ovat samankaltaiset tai eri, ja matkustusasiakirjan tiedot ovat samat, mutta biometriset tiedot poikkeavat toisistaan.

Artiklassa 31 säädetään vihreästä linkistä. EU:n tietojärjestelmien olevien tietojen välinen linkki luokitellaan vihreäksi, jos linkitetyillä tiedoilla a) ei ole samoja biometrisiä henkilötietoja, mutta henkilöllisyystiedot ovat samat tai jos linkitettyjen tietojen on todettu koskevan kahta eri henkilöä rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaavan viranomaisen toimesta, b) ei ole samoja biometrisiä henkilötietoja ja henkilötiedot ovat samankaltaiset tai eri sekä matkustusasiakirjan tiedot ovat samat, ja linkitettyjen tietojen on todettu koskevan kahta eri henkilöä a-kohdassa mainitun viranomaisen toimesta, c) on samat matkustusasiakirjan tiedot, mutta eri henkilöllisyystiedot eikä asianomaisesta henkilöstä ole biometrisiä tietoja missään EU:n tietojärjestelmistä ja edellisissä kohdissa mainittu viranomainen on todennut tietojen koskevan kahta eri henkilöä.

Artiklassa 32 säädetään punaisesta linkistä. Kahden tai useamman EU:n tietojärjestelmän tietojen välinen linkki luokitellaan punaiseksi, kun linkitetyillä tiedoilla on a) samat biometriset tiedot, mutta henkilöllisyystiedot ovat joko samankaltaiset tai eri ja rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaava viranomainen on todennut, että tiedot koskevat perusteettomasti samaa henkilöä, b) samat, samankaltaiset tai eri henkilöllisyystiedot ja samat matkustusasiakirjan tiedot, mutta biometriset tiedot ovat eri ja a-kohdassa mainittu viranomainen on todennut linkitettyjen tietojen koskevan kahta eri henkilöä, joista ainakin toinen käyttää samaa matkustusasiakirjaa luvattomasti, c) samat henkilöllisyystiedot mutta eri biometriset tiedot ja matkustusasiakirjan tiedot joko puuttuvat tai ovat eri, minkä lisäksi a-kohdassa mainittu viranomainen on todennut, että tiedot koskevat perusteettomasti kahta eri henkilöä, d) eri henkilöllisyystiedot mutta samat matkustusasiakirjan tiedot ja yhdessäkään EU:n tietojärjestelmässä ei ole henkilön biometrisiä tietoja ja a-kohdassa mainittu viranomainen on todennut tietojen koskevan perusteettomasti samaa henkilöä.

Viranomaisella on velvollisuus ilmoittaa asianomaiselle henkilölle lainvastaisten rinnakkaisten henkilötietojen olemassaolosta ja annettava tunnistenumero, viittaus rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaavaan viranomaiseen sekä verkkoportaalin osoite. Säädetty ei kuitenkaan rajoita SIS-kuulutusten käsittelyä koskevien säädöstenmukaisten rajoitusten

soveltamista, jotka ovat tarpeen turvallisuuden ja yleisen järjestyksen turvaamiseksi, rikosten ehkäisemiseksi ja sen takaamiseksi, ettei mikään kansallinen tutkinta vaarannu.

Artiklassa 33 säädetään tietojen välille luotavasta valkoisesta linkistä, jollainen luodaan kun a) linkitetyillä tiedoilla on samat biometriset tiedot ja samat tai samankaltaiset henkilötiedot, b) henkilötiedot ovat samat tai samankaltaiset ja biometriset tiedot puuttuvat, c) biometriset tiedot ja matkustusasiakirja ovat samat ja henkilöllisyystiedot samankaltaiset ja d) biometriset tiedot ovat samat, mutta henkilöllisyystiedot ovat samankaltaiset tai eri, ja rinnakkaishenkilöllisyyksien todentamisesta vastaava viranomainen on todennut tietojen koskevan samaa henkilöä.

Artiklassa 34 säädetään henkilöllisyydenvahvistustiedostosta, jossa on oltava seuraavat tiedot: artikloissa 30-33 viitatut linkit, viittaus niihin EU:n tietojärjestelmiin, joissa tiedot ovat, tunnistenumero, jolla tiedot ovat saatavissa järjestelmistä, viittaus rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaavaan viranomaiseen ja linkin luonti- ja päivityspäivät. Artiklassa 35 säädetään tietojen säilyttämisestä MID:ssä. Tiedot ja linkit tallennetaan ainoastaan siksi aikaa, kunnes tiedot on tallennettu kahteen tai useampaan EU:n tietojärjestelmään. Tiedot on poistettava MID:stä automaattisesti. ’

Eu-LISA säilyttää lokitiedot kaikista MID:ssä tehdyistä tietojenkäsittelytoimista.

2.1.4 Tietosuoja

Poliisiyhteentoimivuusasetuksen johdanto-osan 53 kappaleen mukaan asetusta (EU) 2016/679 sovelletaan kansallisten viranomaisten tämän asetuksen mukaisen yhteentoimivuuden toteuttamiseksi suorittamaan henkilötietojen käsittelyyn, paitsi jos jäsenvaltioiden nimetyt viranomaiset tai keskusyhteyspisteet käsittelevät tietoja terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi. Johdanto-osan 54 kappaleen mukaan, jos jäsenvaltioiden tämän asetuksen mukaisen yhteentoimivuuden toteuttamiseksi suorittaman henkilötietojen käsittelyn toteuttavat toimivaltaiset viranomaiset terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi, sovelletaan direktiiviä (EU) 2016/680. Johdanto-osan 57 kappaleen mukaan asetusta (EU) 2018/1725 sovelletaan eu-LISAn ja muiden unionin toimielinten ja elinten suorittamaan henkilötietojen käsittelyyn niiden hoitaessa tämän asetuksen mukaisia tehtäviään, sanotun kuitenkaan rajoittamatta asetuksen (EU) 2016/794 soveltamista, ja viimeksi mainittua sovelletaan henkilötietojen käsittelyyn Europolissa. Vastaavasti asetusta (EU) 2016/679, asetusta (EU) 2018/1725 tai tapauksen mukaan direktiiviä (EU) 2016/680 sovelletaan 55 kappaleen mukaan asetuksen nojalla toteutettaviin henkilötietojen siirtoihin kolmansiin maihin tai kansainvälisille järjestöille. Lisäksi tietosuojaa koskevia asetuksen (EU) 2018/1862 ja Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/816 erityissäännöksiä sovelletaan johdanto-osan 56 kappaleen mukaan henkilötietojen käsittelyyn näillä asetuksilla säännellyissä järjestelmissä.

Luku VII käsittelee tietosuojaa. Artiklassa 40 säädetään rekisterinpitäjästä. Yhteisessä biometrisessä tunnistuspalvelussa (BMS) olevien tietojen käsittelystä vastaavat ne jäsenvaltioiden viranomaiset, jotka vastaavat Eurodac-, SIS- ja ECRIS-TCN -järjestelmiin tallennetuista biometrisistä malleista. Kohdassa 2 säädetään henkilötietojen käsittelystä CIR:ssä vastaavista viranomaisista. MID:ssä olevien tietojen rekisterinpitäjiä ovat Euroopan raja- ja merivartiosta suhteessa ETIAS-keskusyksikössä tapahtuvaan henkilötietojen käsittelyyn sekä ne jäsenvaltioiden viranomaiset, jotka lisäävät tai muuttavat tietoja henkilöllisyysvahvistustiedostoon.

Artiklassa 41 säädetään tietojen käsittelijästä, joka on yhteisessä BMS:ssä, CIR:ssä ja MID:ssä eu-LISA.

Artiklassa 42 säädetään käsittelyn turvallisuudesta. Kohdassa 1 säädetään, että eu-LISA, ETIAS-keskusyksikkö, Europol ja jäsenvaltioiden viranomaiset varmistavat henkilötietojen käsittelyn turvallisuuden asetusta sovellettaessa sekä tekevät yhteistyötä turvallisuuteen liittyvissä tehtävissä. Eu-LISA vastaa yhteentoimivuuskomponenttien ja siihen liittyvän viestintäinfrastruktuurin turvallisuudesta. Lisäksi eu-LISA tekee turvallisuutta ja toiminnan jatkuvuutta koskevat suunnitelmat sekä palautumissuunnitelman.

Jäsenvaltioiden ja unionin virastojen on varmistettava, että jokainen yhteentoimivuuskomponentteihin pääsevä viranomainen noudattaa tässä asetuksessa säädettyä ja tekee tarvittaessa yhteistyötä valvontaviranomaisten kanssa. Lisäksi on säädetty rekisterinpitäjän sisäisestä valvonnasta. Artiklassa 45 on säädetty asetuksen vastaisen tietojen käsittelyn seuraamuksista, jotka määrätään kansallisen oikeuden mukaisesti.

Henkilö tai jäsenvaltio, jolle on koitunut aineellista tai aineetonta vahinkoa jäsenvaltion, Europolin, Euroopan raja- ja merivartioviraston tai eu-LISAn tekemästä lainvastaisesta tämän asetuksen vastaisesta toimesta, on oikeutettu korvauksiin kyseiseltä jäsenvaltiolta tai virastolta. Jäsenvaltio tai virasto vapautuu tästä vastuusta osittain tai kokonaan jos se osoittaa, ettei ole vastuussa vahingon aiheutumisesta.

Artiklassa 47 säädetään henkilötietojen keräämisen kohteena olevan tiedonsaantioikeudesta BMS:n, CIR:n ja MID:n osalta. Tiedot on annettava selkeällä ja henkilön ymmärtämällä kielellä sekä alaikäisille henkilöille ikätason mukaisesti. Lisäksi sovellettaviin unionin tietosuojasääntöihin sisältyvää tiedonsaantioikeutta koskevia sääntöjä sovelletaan ECRIS-TCN:ään tallennettuihin ja tätä asetusta sovellettaessa käsiteltäviin henkilötietoihin.

Artiklassa 48 säädetään oikeudesta saada pääsy MID:hen tallennettuihin henkilötietoihin ja oikaista ja poistaa ne sekä rajoittaa niiden käsittelyä.

Artiklassa 49 säädetään verkkoportaalin perustamisesta. Verkkoportaalin tarkoitus on helpottaa henkilötietoihin pääsyä, tietojen oikaisemista tai poistamista tai niiden käsittelyn rajoittamista koskevan oikeuden käyttämistä.

Artiklassa 51 on säädetty valvontaviranomaisten harjoittamasta valvonnasta. Jäsenvaltioiden on varmistettava, että sen viranomaiset käsittelevät henkilötietoja asetuksessa säädetyllä tavalla lainmukaisesti. Asetuksen 4 artiklan 4 kohdan määritelmän mukaan valvontaviranomaisilla tarkoitetaan asetuksen (EU) 2016/679 51 artiklan 1 kohdassa tarkoitettua valvontaviranomaista ja direktiivin (EU) 2016/680 41 artiklan 1 kohdassa tarkoitettua valvontaviranomaista.

Artiklan 52 mukaan Euroopan tietosuojavaltuutettu varmistaa, että henkilötietojen käsittelytoimien valvontaa tehdään noudattaen kansainvälisiä valvontastandardeja vähintään joka neljäs vuosi. Artiklassa 53 säädetään valvontaviranomaisten ja Euroopan tietosuojavaltuutetun yhteistyöstä.

2.1.5 Eri toimijoiden vastuualueet

Asetuksessa on tarkasti määritelty eri toimijoiden vastuualueet. Eu-LISAn tehtäviin kuuluu varmistaa yhteentoimivuuskomponenttien keskusinfrastruktuurin toimivuus asetuksessa määritellyllä tavalla, yhteentoimivuuskomponenttien ylläpitäminen teknisissä toimipaikoissaan sekä niiden kehittäminen ja mukautukset. Lisäksi eu-LISA määrittelee yhteentoimivuuskomponenttien fyysisen rakenteen sekä kehittää ja toteuttaa ne.

Eu-LISA:n vastuulla ovat myös yhteentoimivuuskomponenttien ja viestintäinfrastruktuurin hallinnointi, tallennettuja tietoja käsittelevän henkilöstön salassapitosäännösten valvonta, tallennettujen tietojen laatutarkastukset sekä teknisen käyttäjäkoulutuksen järjestäminen.

Jäsenvaltioiden vastuulla on liittyminen ESP:n ja CIR:n viestintäinfrastruktuureihin, olemassa olevien kansallisten järjestelmien ja infrastruktuurin integrointi ESP:hen, CIR:ään ja MID;hen sekä muita teknisiä velvoitteita. Jäsenvaltiot vastaavat myös rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta sekä sitoutuvat noudattamaan kunkin tietojärjestelmän henkilötietojen turvallisuutta ja eheyttä koskevia sääntöjä sekä korjaamaan mahdollisesti havaittavat puutteet. Jäsenvaltioiden vastuulla on myös liittää nimetyt viranomaisensa CIR:ään.

Europolin vastuulla on varmistaa tietoihinsa kohdistuvien kyselyjen käsittelyn. Europol myös vastaa ESP:n käytöstä ja pääsystä. Lisäksi Europol pitää yllä listaa tietoihin pääsevästä henkilöstöstä.

ETIAS-keskusyksikön vastuulla ovat rinnakkaishenkilöllisyyksien manuaalinen todentaminen sekä rinnakkaishenkilöllisyyksien tunnistaminen eri järjestelmiin tallennettujen tietojen välillä.

2.1.6 Delegoidut säännökset ja komiteamenettely

Asetuksen artiklassa 69 tarkemmin säädellyllä tavalla komissiolle siirretään valtaa antaa delegoituja säädöksiä. Komissiota avustaa komitea, jossa jäsenvaltiot ovat edustettuina.

Komissio voi antaa delegoituja säädöksiä asetusten 28 artiklan 5 kohdan, 39 artiklan 5 kohdan, 49 artiklan 6 kohdan, 63 artiklan 2 kohdan ja 65 artiklan 8 kohdan nojalla.

Artiklassa 28 säädettään rinnakkaishenkilöllisyyksien tunnistuksen tuloksista. Sen 5 kohdan nojalla komissio antaa delegoituja säädöksiä, joilla vahvistetaan menettelyt sellaisten tapausten määrittämiseksi, joissa henkilöllisyystietojen voidaan katsoa olevan samat tai samankaltaiset.

Artiklassa 39 säädetään raportoinnin ja tilastoinnin keskustietoarkistosta (CRRS). Sen 5 kohdan mukaan komissio delegoidun säädöksen CRRS:n toimintaa koskevista yksityiskohtaisista säännöistä, mukaan lukien erityiset suojatoimet henkilötietojen käsittelyä varten ja tietoarkistoon sovellettavat turvallisuussäännöt.

Artiklalla 49 perustetaan verkkoportaali, jotta voidaan helpottaa henkilötietoihin pääsyä, niiden oikaisemista tai poistamista taikka niiden käsittelyn rajoittamista koskevan oikeuden käyttämistä. Artiklan 6 kohdan mukaan komissio antaa delegoidun säädöksen, jossa vahvistetaan verkkoportaalin ja käyttöliittymän toimintaa, kieliä, joilla verkkoportaalin on oltava saatavilla, ja sähköpostilomaketta koskevat yksityiskohtaiset säännöt.

Artiklassa 63 säädetään ESP:n käyttöön sovellettavasta siirtymäajasta. Artiklan 2 kohdan mukaan komissiolle annetaan valta antaa delegoitu säädös, jolla edellä tarkoitettua määräaikaa jatketaan kerran enintään vuodella, jos ESP:n toimeenpanoa koskeva arviointi osoittaa, että tällainen määräajan jatkaminen on tarpeen erityisesti niiden vaikutusten vuoksi, joita ESP:n käyttöönotolla olisi rajatarkastusten järjestämiseen ja kestoon.

Artiklassa 65 säädetään rinnakkaishenkilöllisyyksien tunnistukseen sovellettavasta siirtymäajasta. Artiklan 8 kohdan mukaan komissiolle annetaan valta antaa delegoitu säädös, jolla edellä tarkoitettua määräaikaa jatketaan kuudella kuukaudella, kuitenkin niin, että määräajan jatkaminen voidaan uusia kaksi kertaa kuudeksi kuukaudeksi kerrallaan.

Delegoituja säädöksiä on annettu kolme. Ensimmäisellä (artikla 28 kohta 5) määritetään tapaukset, joissa henkilötietojen katsotaan olevan samat tai samankaltaiset. Toinen (artikla 39 kohta 5) koskee raportoinnin ja tilastoinnin keskustietoarkiston (CRRS) toimintaa koskevia yksityiskohtaisia sääntöjä. Kolmannella (artikla 49 kohta 6) vahvistetaan verkkoportaalin ja käyttöliittymän toimintaan liittyviä seikkoja, kieliä, joilla verkkoportaalin on oltava saatavilla sekä sähköpostilomaketta koskevat yksityiskohtaiset säännöt. Delegoitujen säädösten valmistelu komitologiamenettelyssä, johon Suomi on osallistunut, päättyi syksyllä 2020 ja säädösten vahvistaminen tapahtuu 2021.

Asetusten mukaan komissiolle on myös siirretty valta antaa täytäntöönpanosäädöksiä. Nämä säädökset voivat koskea:

- ESP:n käyttäjäprofiilien teknisiä yksityiskohtia,

- eritelmiä tekniselle ratkaisulle, jolla mahdollistetaan kyselyjen tekeminen EU:n tietojärjestelmistä, Europolin tiedoista ja Interpolin tietokannoista ESP:n kautta ja ESP-vastausten muotoa,

- teknisiä sääntöjä linkkien luomiseksi MID:ssä EU:n eri tietojärjestelmissä olevien tietojen välillä,

- sen lomakkeen sisältöä ja muotoa, jolla rekisteröidylle ilmoitetaan punaisen linkin luomisesta,

- yhteisen BMS:n suorituskykyvaatimuksia ja suorituskyvyn seurantaa,

- tietojen automaattisia laadunvalvontamekanismeja, -menettelyjä ja -indikaattoreita,

- UMF-standardin kehittämistä,

- turvallisuushäiriöiden yhteydessä käytettäviä yhteistyömenettelyjä ja

- eritelmiä tekniselle ratkaisulle, jolla jäsenvaltiot voivat hallinnoida käyttäjien pääsyä koskevia pyyntöjä.

Täytäntöönpanosäädöksiä on annettu tähän mennessä kahdeksan mutta useampia säädöksiä työstetään edelleen.

Komissiolle on myös siirretty täytäntöönpanovaltaa määrittää ne päivämäärät, jolloin ESP, yhteinen BMS, CIR, MID ja CRRS otetaan käyttöön.

2.1.7 Voimaantulo ja soveltaminen

Asetuksen voimaantulo ja sen soveltamisen aloittaminen on erotettu toisistaan. Asetus julkaistiin EU:n Virallisessa lehdessä 22.5.2019 ja se tuli voimaan tästä kahdenkymmenen päivän päästä.

Yhteentoimivuuskomponentit otetaan kuitenkin käyttöön vasta kun komissio on määrittänyt niille päivämäärät. Vasta yhteentoimivuuskomponenttien käyttöön oton jälkeen EU-tason tietojärjestelmien yhteentoimivuus tulee mahdolliseksi.

Komission aikatauluarvion mukaan yhteentoimivuuskomponenteista otetaan ensin käyttöön yhteinen BMS vuoden 2022 alkupuolella, tämän jälkeen tulisi CIR vuoden 2022 loppupuolella ja sitten ESP ja MID.

Asetuksessa todetaan vielä erikseen, että sitä sovelletaan Eurodacin osalta päivästä, jona uudelleenlaadittua asetusta (EU) N:o 603/2013 aletaan soveltaa.

2.2 Rajayhteentoimivuusasetus

Rajayhteentoimivuusasetus on annettu kehyksen vahvistamiseksi rajoja ja viisumipolitiikkaa koskevien EU:n tietojärjestelmien yhteentoimivuudelle. Näitä tietojärjestelmiä ovat erityisesti VIS, EES ja ETIAS.

Raja- ja poliisiyhteentoimivuusasetusten artiklat ovat muutoin pitkälle yhteneväisiä.

Delegoidut säädökset ja komiteamenettely sekä voimaantulo ja soveltaminen ovat samoja molemmissa asetuksissa.

3 Nykytila ja sen arviointi

EU:n tietojärjestelmät SIS, VIS ja Eurodac eivät tällä hetkellä ole yhteydessä toisiinsa. Tämä tekee järjestelmien käytöstä hajanaista, monimutkaista, hidasta ja vaikeaa. Järjestelmät eivät ole keskenään yhteneviä, mikä tarkoittaa laaja-alaista perehtymis- ja koulutustarvetta, jotta tietojärjestelmiä voidaan hyödyntää täysimääräisesti. Lisäksi tietojärjestelmillä on eri rekisterinpitäjiä, joka vaikuttaa siihen, että esimerkiksi käyttöoikeuksien hallinnointi ei tapahdu keskitetysti. Vaarana on, että kaikkia käytössä olevia tietoja ei huomata tai niitä ei voida täysin hyödyntää kiiretilanteissa. Lainvalvontaviranomaisilla ei ole aina saatavillaan käyttökelpoista tietoa, joka voi osin heikentää kansalasten turvallisuutta ja luoda katvealueita. Edellä mainittujen järjestelmien lisäksi rakenteilla ovat EES-, ETIAS- ja ECRIS-TCN-järjestelmät.

Rajavartijat ja poliisit joutuvat tekemisiin EU:n tasolla monin eri tavoin hallinnoiduista tietojärjestelmistä muodostuvan monimutkaisen kokonaisuuden kanssa. Lisäksi kaikki EU:n jäsenvaltiot eivät ole mukana kaikissa EU:n tietojärjestelmissä. Tietoa pirstaloituu, samaa asiaa hoidetaan useampaa eri tiedonvaihtokanavaa käyttäen, mikä vie resursseja ja voi aiheuttaa sekaannusta. Tällä hetkellä erityyppisiä kansainvälisen ja eurooppalaisen rikostorjuntayhteistyön kanavia on lukuisia, jotka pääosin täydentävät toisiaan, jossain tapauksissa kanavat nähdään toisensa poissulkevina. EU:n tietojärjestelmien yhteentoimivuus voisi osaltaan merkittävästi poistaa nykyisiä katvealueita, joilla henkilöitä voidaan rekisteröidä eri peitenimillä eri tietojärjestelmiin, jotka eivät ole yhteydessä toisiinsa.

Henkilön tunnistamiseen liittyen poliisimiehellä on tällä hetkellä oikeus poliisilain 2 luvun 1 pykälän perusteella yksittäisen tehtävän suorittamiseksi saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Jos henkilö kieltäytyy antamasta näitä tietoja eikä henkilöllisyyttä voida muutoin selvittää, poliisimiehellä on oikeus selvittää henkilöllisyys henkilötuntomerkkien perusteella. Saman pykälän 3 momentin mukaan poliisimiehellä on oikeus henkilöllisyyden selvittämiseksi ottaa kiinni henkilö, joka kieltäytyy antamasta 1 momentissa tarkoitettuja tietoja tai antaa siinä tarkoitetuista seikoista todennäköisesti virheellisen tiedon, jos kiinniottaminen on välttämätöntä henkilöllisyyden selvittämiseksi.

Kuolemansyyn selvittämisestä annetun lain (459/1973) 7 §:ssä säädetään tilanteista, jolloin poliisin on suoritettava tutkinta kuolemansyyn selvittämiseksi. Kuolemansyyn selvittäminen käsittää niiden tietojen hankkimisen, joiden perusteella voidaan todeta kuolema ja arvioida sen ajankohta, voidaan varmistaa vainajan henkilöllisyys, saadaan käsitys kuolinhetkellä vallinneista olosuhteista ja kuolintapahtumaan liittyvistä seikoista, määritetään kuolinsyy ja -luokka ja laaditaan kuolemansyyn selvittämiseen kuuluvat asiakirjat.

Poliisi vastaa oikeuslääketieteellisen kuolemansyynselvityksestä. Uhrintunnistustoiminta on osa kuolemansyyn selvittämistä. Poliisilla on uhrintunnistus- eli DVI-yksikkö (Disaster Victim Identification), joka suorittaa uhrien tunnistamista muun muassa niissä onnettomuus- tai rikostapauksissa, joissa uhrien lukumäärä on suuri, uhrit ovat vaikeasti tunnistettavia tai uhreja on kateissa. Uhrintunnistusyksikkö avustaa paikallispoliisia tarvittaessa uhrintunnistustoiminnassa uhrien lukumäärästä ja tapauksen luonteesta riippumatta, myös yksittäistapauksissa.

Uhrintunnistusyksikkö suorittaa uhrien tunnistamista tarvittaessa myös sellaisissa tapauksissa, joissa Suomen kansalainen tai kansalaisia on kuollut ulkomailla. Pyydettäessä uhrintunnistusyksikkö voi osallistua tunnistamistehtäviin myös ulkomailla, vaikka Suomen kansalaisia ei olisikaan uhrien joukossa.

Henkilöllisyyden selvittämiseksi rajavartiomiehellä on rajavartiolain 36 §:n 1 momentin mukaan oikeus saada Rajavartiolaitokselle säädetyn yksittäisen tehtävän suorittamiseksi jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Rajavartiomiehellä on myös rajavartiolain 28 §:n 1 momentin 3 kohdan perusteella oikeus rajavalvontaan liittyen, Schengenin rajasäännöstössä tarkoitetun rajavalvonnan suorittamiseksi, suorittaa ilman rikosepäilyä Schengenin rajasäännöstön 8 artiklan 2 kohdassa mainitut toimenpiteet, joihin kuuluu muu muassa henkilöllisyyden ja kansalaisuuden sekä rajanylitykseen oikeuttavan matkustusasiakirjan aitouden ja voimassaolon tarkastaminen. Lisäksi rajavartiomiehellä on rajavartiolain 33 §:n mukaisissa poliisitehtävissä poliisilain 2 ja 3 luvussa tarkoitetut toimivaltuudet.

Tullimiehellä on tullilain (304/2016) 3 luvun 17 §:n nojalla yksittäisen tullitoimenpiteen suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Tullitoimenpiteellä tarkoitetaan tullilain 1 luvun 2 §:n 7 kohdan mukaan kaikkia Tullin tehtäviin kuuluvia virkatoimia tullirikosten esitutkintaa ja rajatarkastusta lukuun ottamatta. Jos henkilö kieltäytyy antamasta edellä mainittuja tietoja tai antaa niistä todennäköisesti virheellisen tiedon, tullimiehellä on henkilöllisyyden selvittämiseksi oikeus ottaa kiinni henkilö, jos kiinniottaminen on välttämätöntä henkilöllisyyden selvittämiseksi. Jos henkilöllisyyttä ei voida muulla tavoin selvittää, on tullimiehellä oikeus selvittää henkilöllisyys henkilötuntomerkkien perusteella.

Tullin rikostorjunnan tullimiehen oikeudesta henkilöllisyyden selvittämiseen säädetään puolestaan rikostorjunnasta Tullissa annetun lain (623/2015) 2 luvun 15 §:ssä. Säännöksen mukaan tullirikostorjunnan tullimiehellä on Tullille säädetyn yksittäisen tehtävän suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Jos tietoja kieltäydytään antamasta ja henkilöllisyyttä ei voida muutoin selvittää, tullirikostorjunnan tullimiehellä on oikeus selvittää henkilöllisyys henkilötuntomerkkien sekä henkilötietojen käsittelystä annetun lain (650/2019) 7 ja 8 §:ssä ja henkilötietojen käsittelystä poliisitoimessa (616/2019) annetun lain 5, 6, 11 ja 12 §:ssä tarkoitettujen tietojen perusteella. Tullimiehellä on lisäksi oikeus henkilöllisyyden selvittämiseksi ottaa kiinni se, joka kieltäytyy antamasta edellä mainittuja tietoja tai antaa näistä seikoista todennäköisesti virheellisen tiedon, jos kiinniottaminen on välttämätöntä henkilöllisyyden selvittämiseksi.

Poliisilla, rajavartijalla ja tullimiehellä on siten jo kattava lakiin perustuva oikeus henkilön henkilöllisyyden tarkistamiseksi. Poliisi- ja rajayhteentoimivuusasetusten 20 artiklan käyttöönotto tehostaisi henkilöllisyyden tunnistamista edelleen ja mahdollistaisi lisäksi sen, ettei henkilöä välttämättä tulisi enää ottaa kiinni asian selvittämiseksi.

Poliisi- ja rajayhteentoimivuusasetusten soveltaminen edellyttää täydentävää kansallista sääntelyä, jos jäsenvaltio haluaa käyttää poliisi- ja rajayhteentoimivuusasetusten artiklassa 20 annettua mahdollista säätää kansallisesti siitä, että asetuksen 4 artiklan 19 kohdassa tarkoitetut poliisiviranomaiset pääsevät yhteiseen henkilöllisyystietovarantoon henkilön tunnistamista varten.

Ehdotetulla lailla täydennetään asetusten säännöksiä siltä osin kuin se on välttämätöntä, jotta kansallisesti voidaan käyttää asetusten antamaa mahdollisuutta henkilön henkilöllisyyden tarkistamiseksi.

Asetuksista aiheutuva täydentävä kansallinen säätely annettaisiin omana lakina, koska sääntely sijoittaminen jo olemassa olevaan lainsäädäntöön ei olisi tarkoituksenmukaista.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

4.1.1 Yhteentoimivuuskomponentit

Poliisi- ja rajayhteentoimivuusasetusten keskeisin ehdotus on neljän yhteentoimivuuskomponenttien perustaminen.

1. Eurooppalainen hakuportaali (ESP), jonka kautta voidaan tehdä samanaikaisia hakuja useissa tietojärjestelmissä ml. biometriset tiedot, kuten kasvokuvat ja sormenjäljet.

2. Yhteinen biometrinen tunnistuspalvelu (yhteinen BMS), jonka avulla yhteen järjestelmään tallennettavat biometriset tiedot ovat vertailukelpoisia muihin järjestelmiin tallennettujen sormenjälkien ja kasvokuvien kanssa.

3. Yhteinen henkilöllisyystietovaranto (CIR), johon tallennetaan EU:n tietojärjestelmiin kuuluvat kolmansien maiden kansalaisten henkilötiedot sekä biometriikkaa ja matkustusasiakirjan tiedot.

4. Rinnakkaishenkilöllisyyksien tunnistin (MID), joka tarkistaa, löytyykö samoilla henkilö-, biometrisilla- tai matkustusasiakirjatiedoilla henkilöitä muista järjestelmistä, jotta voidaan havaita samoihin biometrisiin tietoihin liittyvät rinnakkaishenkilöllisyydet.

Näiden komponenttien avulla EU:n olemassa olevat tietojärjestelmät (SIS, VIS ja Eurodac) sekä rakenteilla olevat (EES, ETIAS ja ECRIS-TCN) tehdään yhteentoimiviksi. Tämä tarkoittaa, sitä, että kyseiset järjestelmät täydentävät toisiaan, jotta voitaisiin helpottaa henkilöiden virheetöntä tunnistamista, mukaan lukien tuntemattomat henkilöt, jotka eivät pysty osoittamaan henkilöllisyyttään tai tunnistamatta jääneet ihmisten jäännökset. Lisäksi tietojärjestelmien yhteentoimivuus edistää henkilöllisyyspetosten torjumista ja parantaa ja yhdenmukaistaa kyseisten EU:n tietojärjestelmissä olevien tietojen laatuvaatimuksia sekä virtaviivaistaa pääsyä EES-, VIS-, ETIAS- ja Eurodac- järjestelmiin terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi ja tukee EES-, VIS-, ETIAS-, Eurodac-, SIS- ja ECRIS-TCN-järjestelmien tarkoituksia.

Yhteentoimivuuskomponenteista säädetään poliisi- ja rajayhteentoimivuusasetuksissa. Säädökset eivät edellytä kansallista täydentävää lainsäädäntöä. Kaikki jäsenvaltiot ottavat kunkin yhteentoimivuuskomponentin käyttöön samanaikaisesti.

Biometristen tietojen käyttö

Biometriset tiedot (sormenjäljet, kasvokuva, kämmenjälkitiedot) ovat paljon luotettavampia henkilön tunnistamisessa kuin aakkosnumeeriset tiedot. Samalla biometriset tiedot ovat arkaluonteisia henkilötietoja, jotka kuuluvat EU:n tietosuojalainsäädännössä tarkoitettuihin erityisiin henkilötietoryhmiin.

Olemassa olevista EU-tason tietojärjestelmistä SIS, VIS ja Eurodac sisältävät biometriä tietoja. Myös rakenteilla olevat EES ja ECRIS-TCN tulevat sisältämään biometrisiä tietoja. SIS-järjestelmä on näistä ainoa järjestelmä, jonne voidaan tallentaa myös kämmenenjälkitiedot. SIS-järjestelmä sisältää lisäksi DNA-profiilit. Koska näitä tietoja ei muihin järjestelmiin tallenneta, niin henkilötietojen käsittelyyn liittyvien tarpeellisuus- ja suhteellisuusperiaatteiden mukaisesti kämmenjälkitietoja ja DNA-profiileja ei ole huomioitu eikä käytetä yhteentoimivuuskomponenteissa.

Yhteentoimivuuskomponenteista yhteisen BMS:n tarkoituksena on helpottaa mahdollisesti useisiin EU-tason tietojärjestelmiin rekisteröidyn henkilön tunnistamista. Kaikki automaattiset sormenjälkien tunnistusjärjestelmät käyttävät biometrisiä malleja, jotka on muodostettu tiedoista, jotka on saatu todellisista biometrisistä näytteistä piirteiden erottamisen avulla. Yhteinen BMS kokoaa ja tallentaa yhteen paikkaan kaikki nämä biometriset mallit. Ne pidetään loogisesti toisistaan erotettuina sen mukaan, mistä tietojärjestelmästä tiedot ovat peräisin. Tämä helpottaa järjestelmien välisiä vertailuja biometrisiä malleja käyttäen.

Esityksessä ei ehdoteta muutoksia sääntelyyn, joka koskee kansallisiin rekistereihin tallennettujen biometristen tietojen käsittelyedellytyksiä ja luovuttamista EU:n tietojärjestelmiin.

4.1.2 EU:n tietojärjestelmien väliset linkit

Yhteentoimivuuskomponenteista MID perustetaan, jotta ne henkilöt, joiden henkilötietoja EU:n tietojärjestelmiin on tallennettu, voitaisiin tunnistaa tarkasti.

MID;n tarkoitus on luoda linkkejä EU:n tietojärjestelmissä olevien tietojen välille ja tallentaa ne rinnakkaishenkilöllisyyksien havaitsemiseksi, millä pyrittäisiin sekä helpottamaan vilpittömässä mielessä matkustavien henkilöllisyyden selvittämistä että torjumaan henkilöllisyyspetoksia. MID:ssä olisi ainoastaan oltava linkit useammassa kuin yhdessä EU:n tietojärjestelmässä oleviin henkilöihin. Linkitetyt tiedot rajataan tietoihin, jotka ovat tarpeen sen todentamiseksi, onko henkilö perustellusti tai perusteettomasti kirjattu eri tietojärjestelmiin eri henkilöllisyyksillä, tai sen selvittämiseksi, ovatko kaksi henkilöä, joilla on samankaltaiset henkilöllisyystiedot, kenties eri henkilö.

Linkkejä on neljä erilaista: keltainen linkki, vihreä linkki, punainen linkki ja valkoinen linkki.

Keltaisella linkillä tarkoitetaan sitä, että kahdessa tai useammassa EU-tietojärjestelmässä on tietoja joko eri henkilöistä mutta tiedot ovat joiltain osin yhteneväisiä tai samasta henkilöstä mutta tiedot eri järjestelmissä poikkeavat toisistaan. Tietojen tarkistuksen jälkeen kuitenkin selviää, että kyseessä on eri henkilöt tai sama henkilö mutta tilanteessa ei ole mitään epäselvää eikä rekisteröity henkilö ole antanut vääriä tietoja itsestään.

Vihreällä linkillä tarkoitetaan sitä, että kahdessa tai useammassa EU-tietojärjestelmässä on tietoja eri henkilöistä mutta tiedot ovat joiltain osin yhteneväisiä ja tietojen manuaalisesta todentamisesta vastaava viranomainen on todennut, että linkitetyt tiedot koskevat kahta eri henkilöä.

Punainen linkki tarkoittaa sitä, että kahdessa tai useammassa EU-tietojärjestelmässä on erilaisia tietoja henkilöstä ja tietojen manuaalisesta todentamisesta vastaava viranomainen on todennut, että linkitetyt tiedot koskevat perusteettomasti samaa henkilöä.

Valkoinen linkki tarkoittaa sitä, että kahdessa tai useammassa EU-tietojärjestelmässä on tietoja samasta henkilöstä eikä tiedoissa ole mitään epäselvää.

Linkkejä koskevat säädökset eivät edellytä kansallista täydentävää lainsäädäntöä.

4.1.3 Kyselyjen tekeminen henkilöllisyystietovarannosta (CIR) terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi

Poliisi- ja rajayhteentoimivuusasetusten artikloissa 22 nimetyille viranomaisille annetaan yksittäistapauksessa oikeus tehdä haku CIR:stä, kun se on tarpeen vakavan rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi.

Poliisiyhteentoimivuusasetuksen 22 artiklan mukaan nimetyt viranomaiset ja Europol voivat yksittäistapauksessa tehdä haun CIR:stä, kun on perusteltu syy katsoa, että hakujen tekeminen EU:n tietojärjestelmistä edistää terrorismirikosten tai muiden vakavien rikosten torjumista, havaitsemista ja tutkimista, erityisesti, jos on olemassa epäily siitä, että terrorismirikoksesta tai muusta vakavasta rikoksesta epäilty, tällaiseen rikokseen syyllistynyt tai tällaisen rikoksen uhri on henkilö, jota koskevia tietoja on tallennettu Eurodaciin, saadakseen tiedon siitä, onko Eurodacissa tietoja tietystä henkilöstä.

Rajayhteentoimivuusasetuksen 22 artiklan on samansisältöinen sillä erolla, että se koskee tietoja, jotka on tallennettu EES-, VIS- tai ETIAS-järjestelmään.

Jos kyselyn tuloksena saadaan vastaus, joka osoittaa, että joko Eurodacissa tai EES:ssä, VIS:ssä tai ETIAS-järjestelmässä on tietoja kyseisestä henkilöstä, voidaan vastausta käyttää ainoastaan rajoittamatonta pääsyä koskevan pyynnön esittämiseksi tällaista pääsyä koskevissa säädöksissä vahvistettuja edellytyksiä ja menettelyjä noudattaen. Poliisi- ja raja yhteentoimivuusasetukset eivät siten anna pääsyä edellä mainittuihin tietojärjestelmiin vaan niihin pääsyoikeus määräytyy kyseisen järjestelmän oikeusperustan mukaan. On kuitenkin huomioitava, että jo tieto siitä, että henkilö on rekisteröity johonkin tietojärjestelmään, on henkilötieto.

Poliisi- ja rajayhteentoimivuusasetusten artiklat 22 eivät edellytä kansallista täydentävää lainsäädäntöä.

4.1.4 Pääsy henkilöllisyystietovarantoon (CIR) henkilön tunnistamista varten

Poliisi- ja rajayhteentoimivuusasetusten 20 artikla edellyttää, että jos jäsenvaltio haluaa soveltaa artiklaa, sen tulee antaa tästä kansallista lainsäädäntöä.

Artiklassa poliisiviranomaiselle annetaan mahdollisuus päästä CIR:iin henkilön tunnistamista varten, kun on kyse laittoman maahanmuuton estämisen ja torjumisen edistämisestä tai korkean turvallisuustason edistämisestä unionin vapauden, turvallisuuden ja oikeuden alueella, mukaan lukien yleisen järjestyksen ylläpitäminen ja turvallisuuden takaaminen jäsenvaltioiden alueella. Jäsenvaltioiden on nimettävä toimivaltaiset poliisiviranomaiset ja vahvistettava henkilöllisyyden selvittämisen menettelyt, edellytykset ja kriteerit.

Asetusten mukaan poliisiviranomaisella tarkoitetaan direktiivin (EU) 2016/680

luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 3 artiklan 7 alakohdassa määriteltyä toimivaltaista viranomaista.

Kyseisiä viranomaisia ovat:

a) kaikkia viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvät syytetoimet tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy; tai

b) kaikkia muita elimiä tai yksiköitä, joille on jäsenvaltion lainsäädännössä annettu tehtäväksi käyttää julkista valtaa tai valtuuksia rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syytetoimiin tai rikosoikeudellisten seuraamusten täytäntöönpanoon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy.

Lisäksi jos jäsenvaltio haluaa mahdollistaa, että poliisiviranomainen saa luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa ja yksinomaan sellaisten tuntemattomien henkilöiden tunnistamiseksi, jotka eivät pysty osoittamaan henkilöllisyyttään, tai tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi tehdä kyselyjä CIR:stä kyseisten henkilöiden biometrisillä tiedoilla, sen tulee säätää tästä kansallisella lainsäädännöllä.

Ehdotuksessa esitetään, että Suomi antaisi kansallista lainsäädäntöä poliisi- ja rajayhteentoimivuusasetusten 20 artiklan täytäntöönpanemiseksi. Ehdotetulla lainsäädännöllä täydennetään asetusten säännöksiä siltä osin, kun se on välttämätöntä. Asetuksista aiheutuva täydentävä kansallinen säätely annetaan omana lakina, koska säätelyn sijoittaminen jo olemassa olevaan lainsäädäntöön ei olisi tarkoituksenmukaista ottaen huomioon asetusten tavoite.

Suomessa viranomaisia, joilla annettaisiin pääsy CIR:iin henkilön tunnistamista varten olisivat poliisi, Rajavartiolaitos ja Tulli.

Lisäksi esitetään, että poliisi saisi luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa oikeuden tehdä kyselyjä CIR:iin sellaisten tuntemattomien henkilöiden tunnistamiseksi, jotka eivät pysty osoittamaan henkilöllisyyttään tai tehdä kyselyjä biometrisilla tiedoilla tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi.

4.1.5 Kyselyjen tekeminen ja pääsy CIR:iin muissa tehtävissä

Suomalainen virkamies voi käyttää yhteentoimivuuskehikkoon kuuluvia tietojärjestelmiä eri tarkoituksissa. Esimerkiksi poliisi-, tai tullimies voi suorittaa Schengenin rajasäännöstön mukaista rajatarkastusta ja rajavartiomies rikostorjuntatehtävää. Poliisin rajatarkastustehtävästä ja siihen liittyvistä toimivaltuuksista säädetään poliisilain (872/2011) 2 luvun 21 §:ssä ja Tullin rajatarkastustehtävistä ja -toimivaltuuksista tullilain (304/2016) 31 §:ssä. Pykälien mukaan poliisimiehellä ja tullimiehellä on oikeus rajatarkastuksen toimittamiseen muun muassa rajavartiolain 28 §:ssä rajavartiomiehelle säädetyin toimivaltuuksin.

Pääsyoikeus yhteentoimivuuskehikon sisältämiin tietoihin on tehtäväsidonnainen. Rajatarkastustehtävässä poliisimies, rajavartiomies ja tullimies saavat pääsyoikeuden niihin tiedostoihin, joita yhteentoimivuuskehys sisältää ja joita tarvitaan rajatarkastuksen suorittamiseen.

Järjestelmä antaa pääsyoikeuden tarpeellisiin tietoihin automaattisesti, kun yksilötietuetta tallennetaan EES-järjestelmään. Sama mekanismi pätee myös viisumin myöntöön.

Rikostorjuntatehtävässä sama poliisi-, rajavartio- tai tullimies saa oikeuden tietoihin vain edellä mainittujen 20 ja 22 artiklojen kautta.

4.2 Pääasialliset vaikutukset

4.2.1 Vaikutukset viranomaisten toimintaan

Yhteentoimivuuskokonaisuuden kansallinen toimeenpano ja ohjaus

Sisäministeriö asetti yhteistyössä oikeusministeriön, ulkoministeriön ja valtiovarainministeriön kanssa kansallisen yhteentoimivuushankkeen varmistamaan ja koordinoimaan yhteentoimivuusasetusten täytäntöönpanoa Suomessa.

Hankkeen avulla sovitetaan yhteen kansallinen osallistuminen EU:n keskitettyjen tietojärjestelmien kehittämiseen, niiltä osin kuin linjauksilla on vaikutusta yhteentoimivuuden käytännön toteuttamiseen, sekä varmistetaan yhteentoimivuuden aiheuttamien muutosten oikea-aikainen toimeenpano.

Hanke seuraa myös EU-tason tietojärjestelmien osalta asetettuja kansallisia hankkeita. Vastuu yhteentoimivuuden käytännön toteuttamisesta, kansallisten muutosten ja toimenpiteiden oikea-aikaisesta toimeenpanosta ja niiden resursoinnista on kuitenkin kullakin vastuuviranomaisella (poliisi, Rajavartiolaitos, Tulli, Maahanmuuttovirasto, oikeusrekisterikeskus sekä ulkoministeriö).

Poliisi, Tulli ja Rajavartiolaitos

Uudistuksen myötä EU:n nykyiset ja tulevat tietojärjestelmät ovat yhteydessä toisiinsa. Rajaturvallisuuteen ja sisäiseen turvallisuuteen liittyvä EU:n tietoarkkitehtuuri ei olisi enää hajanainen. Tietojärjestelmien yhteentoimivuutta koskevat asetukset muodostavat yhteyden jo olemassa olevien EU-tietojärjestelmien välille, mahdollistaen henkilötietojen haun yhden portaalin kautta.

Lainvalvontaviranomaisten tiedonhaku helpottuu monella eri tapaa, koska EU:n tietokantoja voidaan käyttää entistä tehokkaammin ja turvallisemmin. Tietojärjestelmien yhteentoimivuus tarjoaa poliisille, Tullille ja Rajavartiolaitokselle näiden pääsyoikeuksia täysimääräisesti kunnioittaen ja tehtäviin liittyviä tarkoituksia varten, mahdollisuuden tehdä hakuja useassa tietojärjestelmässä samanaikaisesti niin, että yhdistetyt tulokset esitetään samassa näkymässä. Lisäksi tietojen eheys paranee, kun mahdolliset syöttövirheet voidaan havaita ja poistaa jo tietoja syötettäessä.

Tiedonhaku on ns. kaksivaiheinen, kun viranomaisen tekemän kysely hakuportaaliin antaa osuman jossakin järjestelmässä, hän voi pyytää kohdennettua pääsyä kyseiseen järjestelmään tätä koskevien sääntöjen ja rajoitteiden mukaisesti. EU tietojärjestelmien yhteentoimivuus ei siten muuta sääntöjä, jotka koskevat pääsyä EU:n tietojärjestelmiin tai käyttötarkoituksen rajoittamista. EU-tietojärjestelmien yhteentoimivuus suoraviivaistaa ja tehostaa viranomaisten pääsyä EU:n tietojärjestelmiin, mutta ei luo uusia toimivaltuuksia itsessään. Käyttöoikeudet perustuvat kunkin tietojärjestelmän oikeusperustaan ja näitä vastaavaan kansalliseen sääntelyyn.

Tullin tutkimissa rikosjutuissa suuri osa rikoksesta epäillyistä on ulkomaan kansalaisia tai Suomessa asuvia muiden maiden kansalaisia. Rikoksia selvitettäessä, todisteita hankittaessa ja näytön keräämisessä tarvitaan usein tietoja siitä, miten henkilö on EU:n ulkorajoilla liikkunut ja onko kiinniotettu henkilö ylipäänsä se henkilö, joka matkustusasiakirjoista ilmenee. Rikostutkinnassa on usein myös tarvetta muodostaa yhteys nopeasti ulkomaan lainvalvontaviranomaisten kanssa ja pyytää suoritettavaksi pakkokeinotoimenpiteitä kiireaikataululla, ettei todisteita hävitetä ja että rikoshyödyn takaisinsaanti voidaan turvata. Tässä EU-tietojärjestelmien yhteentoimivuus helpottaa ja nopeuttaa Tullin suorittamaa rikostutkintaa mahdollistamalla henkilötietojen haun yhden portaalin avulla.

Paljastavan toiminnan puolella Tullissa kohdehenkilöön liittyviä tietoja yhdistetään analyysissa useista eri tietolähteistä. Paljastavassa toiminnassa EU:n tietojärjestelmien yhteentoimivuudella voidaan varmistaa kohdehenkilön riittävä oikeusturva, kun henkilöllisyys saadaan luotettavasti varmistettua perusoikeuksia rajaavia toimenpiteitä suoritettaessa.

Tullin kansainvälisen kaupan ja tavaraliikenteen valvonnan yhtenä tehtävänä on taata unionin ja siellä asuvien henkilöiden turvallisuus. Unionin tullikoodeksin (952/2013) 3 artiklassa säädetään tulliviranomaisten tehtäväksi suorittaa näihin liittyvät toimenpiteet. Tullille on säädetty myös useissa erityislaeissa tavaroiden maahantuontiin ja maastavientiin liittyviä valvontatehtäviä. Esimerkiksi säteilylain (859/2018) 3 luvun 16 §:ssä säädetään Tullin valvontatehtävistä säteilylähteiden ja radioaktiivisten jätteiden tuonnissa ja viennissä. Tavaralähetysten tarkastamisen yhteydessä voidaan joutua selvittämään tavaroita kuljettavan henkilöllisyys. Erityisesti henkilöllisyyden selvittäminen on tarpeen silloin, kun matkustajan epäillään tuovan kehossaan maahan kiellettyjä aineita. Tällöin ei välttämättä ole aloitettu vielä rikoksen esitutkintaa, sillä tullilain 3 luvun 18 §:n 3 momentin mukaan pakkokeinolain 8 luvun 30 §:ssä tarkoitettu henkilönkatsastus tai henkilöntarkastus voidaan suorittaa henkilölle ilman esitutkinnan aloittamista, kunhan vain säädetyt edellytykset täyttyvät. Henkilöllisyyden luotettava selvittäminen EU:n yhteisestä tietojärjestelmästä voi vähentää tarvetta puuttua tarpeettomasti tullitarkastusten kohteiksi valikoitujen henkilöiden perusoikeuksiin, jonka lisäksi tullitarkastusten toimittaminen nopeutuu, mistä voi olla suurikin hyöty esimerkiksi matkustajille.

EU-tietojärjestelmien yhteentoimivuus edellyttää manuaalista MID:ssä muodostuneiden linkkien eli henkilöllisyyksien varmentamista SIS:n osalta. Kun kyse on siis SIS-järjestelmän linkeistä kuulutuksiin henkilöistä, joita etsitään kiinniottoa ja eurooppalaisen pidätysmääräyksen tai luovutussopimuksen perusteella tapahtuvaa luovuttamista varten, kadonneista tai haavoittuvassa asemassa olevista henkilöistä, henkilöistä, joita etsitään oikeudelliseen menettelyyn osallistumista varten, tai henkilöistä salaista tarkkailua tai tiedustelutarkastuksia varten, kuulutuksen tehneen jäsenvaltion SIRENE-toimiston olisi oltava rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaava viranomainen. Suomen SIRENE-toimisto on sijoitettu keskusrikospoliisiin.

Linkit voivat muodostua SIS-kuulutuksen ja minkä tahansa muun yhteentoimivuus-kokonaisuudessa olevan tietojärjestelmän välille. Tämä tarkoittaa sitä, että Suomen syöttämän henkilökuulutuksen ja toisen jäsenvaltion syöttämän, esimerkiksi EES-tiedon välille voi syntyä linkki eli niiden määrä ei ole riippuvainen Suomen kuulutusten määrästä suoraan.

Tiedon tehokas yhdistäminen, analysointi, kerääminen ja jakaminen nykyaikaisilla välineillä ja päivitetyllä lainsäädännöllä on ensiarvoisen tärkeää. Rajat ylittävän rikollisuuden torjunta onnistuu ainoastaan, jos lainvalvontaviranomaisten tietojenvaihto toimii reaaliaikaisesti, sujuvasti ja ilman prosesseihin liittyvää turhaa byrokratiaa. Asetuksilla vastataan osin kansainvälistä poliisiyhteistyötä koskeviin haasteisiin mahdollistamalla ja tehostamalla moniviranomaisyhteistyön malleja ja järjestelmiä.

Poliisiviranomaisen pääsy CIR:iin 20 ja 22 artiklojen mukaisesti olisi uusi työkalu henkilön henkilöllisyyden selvittämisessä. Siten yhteentoimivuusasetuksen myötä henkilön tunnistaminen helpottuu ja nopeutuu eikä kiinniottamisen kaltainen perusoikeuksiin puuttuminen ole välttämättä tarpeen.

Maahanmuuttovirasto

Maahanmuuttoviraston toimintaan vaikuttavia tehtäviä ovat rajayhteentoimivuusasetuksen 21, 26 ja 29 artikloiden mukaisten keltaisten linkkien ja henkilöllisyyden manuaaliseen todentamiseen liittyvät tehtävät tietyissä tilanteissa. Mahdollisia vaikutuksia voi tulla myös esimerkiksi avunannosta muille viranomaisille heidän asetuksista seuraavien tehtävien hoitamista varten.

Merkittävimmät muutokset liittyvät Maahanmuuttoviraston eräiden rekisterihakujen ja tietojen verifiointien keskittämiseen ESP:n kautta. Maahanmuuttovirastolla on jatkossa oltava pääsy tekemään hakuja ainakin VIS-, EES-, ETIAS-, SIS- ja Eurodac järjestelmien tietoihin ESP:tä hyödyntäen. Maahanmuuttovirasto on suunnitellut toteuttavansa nämä haut mahdollisimman pitkälle automatisoidusti ja integroituvansa tältä osin myös poliisin Renki-järjestelmään.

Ulkoministeriö

Ulkoministeriön hallinnonalalla tietojärjestelmien yhteentoimivuuskokonaisuus tulee aiheuttamaan merkittäviä prosessi- ja järjestelmämuutoksia kansalliseen viisumitietojärjestelmään (VISA-viisumijärjestelmä). Teknisesti, VISA tulee integroida yhteentoimivuuskomponettien (ESP, CIR) kanssa. Lisäksi tulee huomioida VIS-järjestelmän rajapinta- sekä prosessimuutokset. Viisumihakemusten käsittelyssä ja teknisessä toteutuksessa on huomioitava tilanteet, joissa henkilötietojen tallennuksen yhteydessä käynnistynyt MID on palauttanut rinnakkaishenkilöllisyyksiä (linkkejä) useammasta järjestelmästä.

Oikeusrekisterikeskus

ECRIS TCN asetus (EU 2019/816) on tullut voimaan 11. kesäkuuta 2019. Asetuksessa säädetään EU jäsenvaltiossa rikostuomion saaneiden kolmansien maiden kansalaisten tunnistetietoja sisältävän keskitetyn tietojärjestelmän perustamisesta. Samaan aikaan tuli voimaan rikosrekisteritietojen EU vaihtoa koskevaa puitepäätöstä muuttava ja ns. ECRIS - päätöksen korvaava direktiivi (EU 2019/884).

Tietojenvaihto ECRIS -järjestelmässä tapahtuu jäsenvaltioiden keskusviranomaisten välityksellä. Suomessa keskusviranomaisena toimii Oikeusrekisterikeskus, jolla nykyisinkin on keskeinen asema jäsenvaltioiden välisessä rikosrekisteritietojen vaihtoon liittyvässä yhteistyössä. Keskitetty, kolmansien maiden kansalaisten tunnistetietoja sisältävä ECRIS-TCN-järjestelmä otetaan käyttöön loppuvuonna 2022. Poliisiyhteentoimivuusasetuksen artiklan 29 kohtien 1-3 perusteella Oikeusrekisterikeskus vastaa kansallisesti rinnakkaishenkilöllisyyksien manuaalisista todentamisista vastaavuuksissa, jotka tuotetaan, kun tietoja tallennetaan ECRIS-TCN:ään tai niitä muutetaan ECRIS TCN asetuksen 5 tai 9 artiklan mukaisesti. Oikeusrekisterikeskus ei kuitenkaan lukeudu kansallisesti toimivaltaiseksi poliisiviranomaiseksi artiklan 20 mukaisissa tunnistamistehtävissä.

Yhteistyö ja tiedonvaihtokanavat kansallisten esitutkintaviranomaisten, SIRENE-toimiston ja muiden rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaavien viranomaisten välillä tulee varmistaa.

4.2.2 Taloudelliset vaikutukset

Yhteentoimivuusasetukset edellyttävät muutoksia kansallisiin tietojärjestelmiin, jotka koskevat useampaa hallinnonalaa sekä virastoa (Poliisihallitus, Rajavartiolaitos, Maahanmuuttovirasto, Tulli, ulkoministeriö, oikeusministeriö ja Oikeusrekisterikeskus). Tämän lisäksi tulee huolehtia tarvittavista tietoverkkoympäristöjen muutoksista. Teknisten muutosten lisäksi yhteentoimivuusasetukset aiheuttavat muutoksia myös näiden viranomaisten toimintoihin ja henkilöstöresursseihin.

Yhteentoimivuusasetuksista aiheutuvia määrärahatarpeita on käsitelty osana julkisen talouden suunnitelman 2022 - 2025 valmistelua sekä osana vuoden 2021 lisätalousarvioiden ja vuoden 2022 talousarvion valmistelua.

EU-tietojärjestelmien kansallista toimeenpanoa ja kehittämistä on tuettu sisäisen turvallisuuden rahastosta (ISF) ohjelmakaudella 2014-2020. Komissio osoitti jäsenvaltioille lisärahoitusta EU-tietojärjestelmiin (EES, ETIAS, SIS III ja yleinen ICT-kehittäminen). Suomen osuus lisärahoituksesta oli yhteensä noin 13,3 miljoonaa euroa. Yhteentoimivuus kuuluu ohjelmakaudella 2021-2027 EU:n sisäasioiden rahastojen soveltamisalaan. Rahastojen kansallisia ohjelmia kaudelle 2021-2027 valmistellaan ja rahastoja hyödynnetään yhteentoimivuusasetusten toimeenpanossa mahdollisuuksien mukaan.

Viranomaisten määrärahatarve on tämän hetken arvioiden mukaan yhteensä 21,5 milj. jakautuen alla olevasti:

Poliisihallinto

Keskusrikospoliisiin sijoitetun SIRENE-toimiston työmäärä tulee lisääntymään, koska se tulee toimimaan rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta vastaavana viranomaisena. EU-tietojärjestelmiin laadittujen kuulutusten väliset linkit voivat muodostua SIS-kuulutuksen ja minkä tahansa muun yhteentoimivuus-kokonaisuudessa olevan tietojärjestelmän välille. Tämä tarkoittaa sitä, että Suomen syöttämän henkilökuulutuksen ja toisen jäsenvaltion syöttämän, esimerkiksi EES-tiedon välille voi syntyä linkki eli niiden määrä ei ole riippuvainen Suomen kuulutusten määrästä suoraan.

SIS:stä annetussa hallituksen esityksessä (HE 35/2021 vp) todetaan, että SIS-järjestelmään syötettäviin kuulutuksiin ei voitaisi enää kansallisen sääntelyn puitteissa lisätä kansallisiin rekistereihin ulkomaalaislain (301/2004), passilain (671/2006) tai henkilökorttilain (663/2016) nojalla talletettuja biometrisia tunnisteita mm. palautus- ja maahantulokieltokuulutuksiin. Biometristen tunnisteiden puuttuminen SIS-kuulutuksista tulee aiheuttamaan enemmän lisätiedonvaihtopyyntöjä sekä lisäämään työmäärää yhteentoimivuuden puitteissa manuaalisesti tarkastettavien linkkien käsittelyn osalta SIS:n ja muiden EU:n tietojärjestelmien välillä.

Manuaalisesti tarkastettavaksi tulevien linkkien määrää ja tästä aiheutuvia taloudellisia vaikutuksia on tässä vaiheessa vaikea arvioida, koska taustalla vaikuttavat sekä eu-LISA:n tekniset ratkaisut kuin myös linkkien volyymi.

Arviota tai tarkennettua tietoa manuaalisesti käsiteltäväksi tulevien linkkien määrästä ei vielä ole. Ehdotuksella on mahdollisesti merkittäviäkin resurssivaikutuksia lisääntyneenä työmääränä.

Rajavartiolaitos

Rajavartiolaitoksella on käynnissä kaksi suurta EU-tietojärjestelmäuudistusta, rajanylitystietojärjestelmä EES ja Euroopan matkustustieto- ja -lupajärjestelmä ETIAS, jotka on tarkoitus ottaa käyttöön 2022. EES:n käyttöönotto muuttaa merkittävästi kansallista rajatarkastusprosessia. Osa yhteentoimivuusasetuksen edellyttämistä teknisistä muutoksista voidaan huomioida EES- ja ETIAS-järjestelmien kehittämisessä, mutta yhteentoimivuuskomponenttien käyttöönotto edellyttää myös merkittäviä muutoksia kansalliseen rajatarkastussovellukseen, jotta se tukee tarvittavia kyselyitä, palautuneet tiedot voidaan käsitellä tarkoituksenmukaisesti ja muun muassa saadaan linkitettyä tarvittavat yksilötiedot.

Merkittävin taloudellisia vaikutuksia aiheuttava muutos yhteentoimivuusasetuksen käyttöönotossa liittyy työmäärän kasvamiseen. Vuonna 2019 eli viimeisenä korona-pandemiaa edeltäneenä vuonna Suomen ulkorajan ylitti yhteensä 16,78 miljoonaa henkilöä. Näistä 10,52 miljoonaa oli ulkomaalaisia, joiden tiedot tallennetaan yhteentoimivuuskehikkoon kuuluviin tietojärjestelmiin, erityisesti EES:iin, VIS:iin ja ETIAS:een. Keltaisten linkkien manuaalinen selvittäminen tulee lisäämään rajatarkastajien työmäärää ja ESP:n sekä MID:n käyttö saattaa pidentää rajatarkastuksen kestoa, jolloin Suomen rajanylityspaikkojen läpäisykapasiteetti pienenee. Läpäisykapasiteetin säilyttäminen nykyisellä tasolla edellyttäisi henkilöstömäärän lisäämistä ja rajanylityspaikkojen rakenteellista kehittämistä.

Tässä vaiheessa Rajavartiolaitoksella ei ole vielä riittäviä perusteita arvioida linkkien selvitystyöstä aiheutuvaa työmäärän kasvua tai ESP:n ja MID:n toiminnasta aiheutuvaa prosessin hidastumista. Ensimmäiset arviot voidaan tehdä aikaisintaan, kun komponenttien kehitystyö on edennyt prototyyppi- tai testausasteelle. Manuaalisen työn määrään vaikuttavat useat seikat, jotka liittyvät muun muassa ensimmäistä kertaa Schengen-alueelle saapuvien määrään, siihen onko kyse viisumivapaista vai viisumivelvollisista matkustajista, MID:n käyttämän vertailumekanismin toimivuuteen/luotettavuuteen, MID:iin asetettavista raja-arvoista, joilla määritetään miten suurta yhdenmukaisuutta tarkoittaa sama, samankaltainen ja erilainen sekä yksityiskohtaiseen prosessiin, jolla manuaalisesti selvitetään keltaisen linkin peruste, ja sen kestoon.

Toiminnallisuuksien käyttöönotosta johtuvat muut kuin tekniset lisätarpeet käsitellään osana Rajavartiolaitoksen toiminnan ja talouden suunnittelua.

Tulli

Yhteentoimivuusasetukset edellyttävät muutoksia myös Tullin tietojärjestelmiin. Tässä vaiheessa taloudellisten vaikutusten arvioiminen ei ole vielä mahdollista luotettavalla tavalla, sillä kaikkia kokonaisuuteen liittyviä osajärjestelmiä ei ole vielä saatu valmiiksi ja taloudelliset vaikutukset jakautuvat eri osajärjestelmien sekä yhteentoimivuusasetusten välillä. Järjestelmän käyttöönotosta aiheutuu taloudellisia vaikutuksia lähinnä järjestelmän ylläpitämisestä sekä henkilöstön kouluttamisesta käyttämään järjestelmää. Tullin osalta olettama on, että EU-tietojärjestelmien yhteentoimivuus nopeuttaa prosesseja sekä vähentää manuaalista selvitystyötä ja sitä kautta tuo taloudellisia säästöjä pitkällä aikavälillä.

Maahanmuuttovirasto

Yhteentoimivuusasetuksista Maahanmuuttovirastolle aiheutuvat taloudelliset vaikutukset liittyvät pääosin tietojärjestelmämuutoksiin ja niiden toteuttamiseen liittyviin henkilöstökustannuksiin. Lisäksi Maahanmuuttovirasto on arvioinut EU:n yhteisiin tietojärjestelmiin ja niiden hallintaan liittyväksi pysyväksi henkilöstön lisäystarpeeksi yhden henkilötyövuoden vuodesta 2026 alkaen.

Ulkoministeriö

Ulkoasiainhallinnon työmäärä kasvaa johtuen rinnakkaishenkilöllisyyksien todentamisesta ja niitä koskevien linkkien manuaalisesta selvittämisestä. Linkkien määrää ja tästä aiheutuvaa lisäresurssoinnin tarvetta on tässä vaiheessa vaikea arvioida. Taloudellisia vaikutuksia ulkoasiainhallinnolle aiheutuu ennen muuta tietojärjestelmän kehittämistyöstä, eu-LISA:n edellyttämiin virallisiin testauksiin osallistumisesta sekä kansallisesta testauksesta.

Oikeusministeriö

ECRIS-TCN-järjestelmää käytetään ESP:n kautta tietyissä käyttötapauksissa. ESP:iin liittyminen kansallisesti edellyttää Oikeusrekisterikeskukselta CRIS-tietojärjestelmän kehitykseen ja yhteentoimivuuteen liittyviä toimenpiteitä. Tavoitteena on mahdollistaa IO-kokonaisuuteen kuuluvan ESP:n käyttö ECRIS-TCN:n hakujen yhteydessä käyttämällä kansallista CRIS-järjestelmää hakujen tekemiseen. Toiminnallisuuden tulisi olla käyttövalmis ECRIS-TCN-järjestelmän käyttöönoton yhteydessä vuosina 2022-2023. Toistaiseksi ei ole tarkasti tiedossa, millaisia tietojärjestelmämuutoksia ESP:iin liittyminen edellyttää ja siten kustannusten suuruutta on vielä tarkennettava IO-hankkeen edetessä. Myös muiden yhteentoimivuuskomponenttien käyttöönotto edellyttää muutoksia etenkin kansalliseen CRIS-järjestelmään sekä integraatioita CIR:ään ja MID;hen. Lisäksi Oikeusrekisterikeskuksen työmäärä kasvaa johtuen rinnakkaishenkilöllisyyksien manuaalisesta todentamisesta sekä turvallisuushäiriöiden käsittelystä asetusten 43 artikloissa edellytetyllä tavalla, mutta näistä aiheutuvaa mahdollista lisäresursoinnin tarvetta on tässä vaiheessa vaikea arvioida.

Yhteentoimivuutta koskevien asetusten täytäntöönpanosta seuraa jonkin verran lisää valvontatehtäviä tietosuojavaltuutetulle. Erityisesti lisätyötä aiheutuisi yhteentoimivuuskomponentteihin kansallisesti siirrettyjen ja sieltä kansallisesti käsiteltävien tietojen valvonnasta. Vaikka kyseisten yhteentoimivien EU tietojärjestelmien valvonta onkin pääosin Euroopan tietosuojavaltuutetun valvonnassa, lisääntyvät kansallisten viranomaisten tehtävät erityisesti lainsäädäntöratkaisuista ja teknisten ratkaisujen luonteesta johtuen. Jonkin verran vaikutuksia olisi myös EU:n valvontaviranomaisten yhteistyöllä. Alustavan arvion mukaan täytäntöönpanosta aiheutuisi lisätyötä enintään 1 henkilötyövuoden verran.

4.2.3 Tiedonhallinnan muutosvaikutukset

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jäljempänä tiedonhallintalaki) säädetään muun muassa tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta. Tiedonhallintalailla varmistetaan viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi.

Poliisi valmistelee yhteistä Renki-nimistä hakukäyttöliittymää kansallisiin tarpeisiin. Tarkoitus on, että tämän liittymän kautta loppukäyttäjä saa pääsyn niihin tietojärjestelmiin, joihin hänellä on lakisääteinen oikeus tekemällä yhden haun. Yhteentoimivuusasetusten edellyttämä pääsy ESP:hen on tarkoitus integroida Renkiin.

Yhteentoimivuus asetusten vuoksi Rajavartiolaitoksen tietojärjestelmissä joudutaan kehittämään rajatarkastussovellusta ja sen ominaisuuksia, jotta ne tukevat yhteentoimivuusasetuksen edellyttämiä toimintoja paitsi tehtävien keskitettyjen kyselyjen ja niiden tuottamien vastausten muutosten osalta, myös toteuttamaan uusia ominaisuuksia saatujen vastausten käsittelyn kannalta. Muutokset liittyvät henkilöllisyyttä koskevien linkkien käsittelyyn, sanoma- ja yhteysmuutoksiin ESP-hakujen osalta sekä tiedonvälitysratkaisuihin linkkien käsittelyjen osalta.

Ratkaisuissa tullaan hyödyntämään EES- ja ETIAS-vaiheissa toteutettuja ratkaisuja sekä olemassa olevia toteutuksia siinä määrin kuin mahdollista, mutta muutoksia joudutaan tekemään RATAS-rajatarkastussovellukseen sekä Ulkonet-kyselyjärjestelmään ESP-kyselyjen toteutuksen osalta. Olemassa olevien toteutusten lisäksi soveltuvin osin jatketaan järjestelmien ja tiedonhallintaan liittyvien ratkaisujen osalta yhteistyötä ja yhteiskäyttöä muiden viranomaisten kanssa, esimerkiksi Rengin käytön osalta.

Tulli tulee liittymään ESP:hen Renki-järjestelmän välityksellä poliisin tavoin. Tullilla on jo olemassa käyttöoikeus Renki-järjestelmään ja järjestelmää käytetään samoin tavoin kuin poliisi omiin toimivaltuuksiin. Tullissa tullaan tulevina vuosina uusimaan tietojärjestelmiä ja tällöin myös liittyminen ESP:hen tullaan arvioimaan uudelleen.

Ulkoministeriössä tullaan toteuttamaan VISA-viisumijärjestelmään muutoksia ja uusia ominaisuuksia, jotta ne tukevat yhteentoimivuusasetusten edellyttämiä toimintoja. VISA-järjestelmä kautta on mahdollista käynnistää haku useaan tietojärjestelmään uuden ESP-hakuportaalin kautta, loppukäyttäjän oikeuksien mukaisesti. Lisäksi järjestelmään toteutetaan rinnakkaishenkilöllisyyttä koskevien linkkien käsittely ja tietojen välittäminen. Näiden toimintojen toteuttaminen edellyttää sanoma- ja yhteysmuutoksia VISA-järjestelmän sekä uusien keskusjärjestelmäkomponenttien välille. Tietojen käsittelyyn ja näyttämiseen toteutettavat toiminnot ja prosessit suunnitellaan niin, että ne tehokkaasti tukevat VISA-järjestelmää käyttäviä viranomaisia.

Maahanmuuttoviraston toimialalla tietojärjestelmien yhteentoimivuuskokonaisuus tulee aiheuttamaan merkittäviä prosessi- ja järjestelmämuutoksia ulkomaalaisasioiden asiankäsittelyjärjestelmä UMA:an.

Esityksessä ei ehdoteta muutoksia voimassa olevaan asiakirjojen julkisuutta ja salassapitoa koskevaan sääntelyyn.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Yhteentoimivuusasetukset ovat suoraan sovellettavaa oikeutta. Asetusten artiklassa 20 säädetään pääsystä CIR:iin henkilön tunnistamista varten. Artiklan mukaan pääsy on mahdollista saada kahdessa erilaisessa tilanteessa, joista on säädetty artiklan 1 ja 4 kohdissa. Toimivaltainen viranomainen voi saada pääsyn CIR:iin vain, jos sitä on erikseen säädetty kansallisella lailla. Suomessa esitetään annettavaksi täydentävää kansallista lainsäädäntöä artiklan 20 osalta. Muilta osin asetukset eivät anna mahdollisuutta säätää asiasta kansallisesti.

5.2 Muiden jäsenvaltioiden suunnittelemat tai toteuttamat keinot

Toisilta jäsenvaltioilta tiedusteltiin vuoden 2021 alkupuolella aikovatko ne ottaa käyttöön poliisi- ja rajayhteentoimivuusasetusten artiklan 20 ja antaa sen osalta kansallista lainsäädäntöä.

Ruotsi, Puola, Latvia, Saksa, Belgia ja Kypros ilmoittivat, että ne ovat ottamassa käyttöön yhteentoimivuusasetusten artiklan 20 ja ne antavat kansallista lainsäädäntöä siitä.

Tsekki ja Espanja katsovat, että niiden kansallinen lainsäädäntö on jo riittävä siihen, että toimivaltaiset viranomaiset pääsevät CIR:Iin, Myös Kroatiassa toimivaltaiset viranomaiset pääsevät CIR:iin, vaikka sitä ei ole suorana todettu kansallisessa laissa biometristen tietojen käsittelyssä (Biometric Data Processing Act).

Itävalta, Kypros, Unkari ja Ranska eivät vielä olleet tehneet lopullista päätöstä.

Perussopimusten mukaan Irlannin tulee ilmoittaa halukkuudesta laittaa täytäntöön yhteentoimivuusasetukset (ns. opt-in). Irlannin on tarkoitus näin toimia ja sen jälkeen antaa kansallista lainsäädäntöä, millä mahdollistetaan toimivaltaisten viranomaisten pääsy CIR:ii yhteentoimivuusasetusten artiklan 20 mukaisesti.

6 Lausuntopalaute

7 Säännöskohtaiset perustelut

1 §. *Soveltamisala.* Pykälään ehdotetaan otettavaksi lain soveltamisalaa koskeva säännös. Siitä ilmenee, että laki sisältää täydentävät säännökset poliisi- ja rajayhteentoimivuusasetusten soveltamisesta Suomessa.

2 §. *Toimivaltainen viranomainen*. Pykälässä säädettäisiin toimivaltaisista viranomaisista poliisi- ja raja yhteentoimivuusasetusten 20 artiklassa mainituissa tilanteissa. Artiklassa 20 säädetään pääsystä EU:n yhteiseen henkilöllisyystietovarantoon (CIR) henkilön tunnistamista varten. Artiklassa 20 käytetään termiä poliisiviranomainen ja sen sisältö on määritelty asetusten 4 artiklan kohdassa 19. Määritelmä on hyvin laaja kattaen lainvalvontaviranomaisia sekä oikeusviranomaisia. Tässä laissa käytetään termiä toimivaltainen viranomainen, koska termillä poliisiviranomainen on Suomessa vakiintunut merkitys, mikä ei ole yhteneväinen poliisi- ja rajayhteentoimivuusasetuksissa omaksutun määritelmän kanssa. Suomessa toimivaltaisiksi viranomaisiksi esitetään vain poliisia, Rajavartiolaitosta ja Tullia. Näiden viranomaisten tehtävien hoitaminen voi edellyttää, että henkilön tunnistamiseksi tulee voida tehdä kysely CIR:iin.

CIR:iin tallennetaan tietoja EES-, VIS-, ETIAS-, Eurodac- ja ECRIS-TCN-järjestelmistä. Poliisi- ja rajayhteentoimivuusasetusten mukaan CIR:n olisi tallennettava henkilötiedot, joita edellä mainituissa järjestelmissä olevien henkilöiden tarkempi tunnistaminen edellyttää, mukaan lukien henkilöllisyystiedot, matkustusasiakirjan tiedot ja biometriset tiedot. CIR:ään olisi tallennettava ainoastaan ne henkilötiedot, jotka ovat ehdottomasti tarpeen henkilöllisyyden selvittämiseksi tarkasti. Käytännössä järjestelmä toimii siten, että kun EES-, VIS, ETIAS-, Eurodac- tai ECRIS-TCN -järjestelmään tallennetaan edellä mainittuja tietoja, ne tallentuvat automaattisesti CIR:iin. Yksinomaan CIR:iin ei siis tallenneta tietoja.

Artiklan 20 mukaista tunnistamista voitaisiin hyödyntää esimerkiksi poliisin toiminnassa tilanteissa, joissa henkilön tunnistaminen on tarpeen yksittäisen tehtävän suorittamiseksi ja henkilö kieltäytyy selvittämästä henkilöllisyyttään. Poliisin voidessa käyttää CIR:n tietoja henkilön tunnistamiseksi, tunnistaminen helpottuu ja nopeutuu eikä kiinniottamisen kaltainen perusoikeuksiin puuttuminen olisi välttämättä tarpeen.

Rajavartiolaitoksen toiminnassa artikla 20 mukaista tunnistamista voidaan hyödyntää esimerkiksi tilanteessa, jossa valtakunnan rajalla on havaittu luvaton rajanylitys ja tilanteesta käynnistyvässä etsinnässä tavataan rajan läheiseltä tiestöltä kävelemässä kolmannen maan kansalainen, jolla ei ole esittää matkustusasiakirjaa tai muita henkilöllisyyttä osoittavia asiakirjoja. Käyttämällä CIR:n tietoja voidaan tunnistaa sekä luvallisesti EU-alueella oleskelevia henkilöitä (EES, Eurodac) että myös henkilöitä, joiden pääsy EU-alueelle on kielletty (SIS).

Tulli voisi hyödyntää artiklan 20 mukaista henkilön tunnistamista, kun se olisi tarpeen vaaraa aiheuttavien esineiden tai aineiden lainvastaisen tuonnin, viennin tai kauttakuljetuksen paljastamiseksi tai torjumiseksi. Kyseessä voisivat olla esimerkiksi aseet, vaaraa aiheuttavat kemikaalit, radioaktiiviset jätteet taikka tilanne, jossa henkilön epäillään tuovan kehonsisäisesti laittomia aineita rajan yli ja henkilö kieltäytyy selvittämästä henkilöllisyyttään. Henkilön tunnistaminen yhteisestä henkilötietovarannosta nopeuttaa tunnistamista ja sujuvoittaa tarkastusprosessia.

3 §. *EU:n yhteisen henkilöllisyystietovarannon käyttäminen.* Poliisi- ja rajayhteentoimivuusasetusten artiklan 20 kohdan mukaan, jos jäsenvaltio haluaa antaa poliisiviranomaiselle oikeuden tehdä kyselyn EU:n yhteiseen henkilöllisyystietovarantoon henkilön tunnistamista varten, on tätä koskevassa kansallisessa säädöksessä täsmennettävä tunnistamiselle täsmällinen poliisi- ja rajayhteentoimivuusasetuksen 2 artiklan 1 kohdan b ja c alakohdan mukainen tarkoitus. Kyseisten alakohtien mukaan tällaisia tarkoituksia olisivat laittoman maahanmuuton estämisen ja torjumisen edistäminen sekä korkean turvallisuustason edistäminen unionin vapauden, turvallisuuden ja oikeuden alueella, mukaan lukien yleisen järjestyksen ylläpitäminen ja turvallisuuden takaaminen jäsenvaltioiden alueella.

Pykälän 1 momentissa esitetään, että poliisilla ja Rajavartiolaitoksella olisi oikeus henkilön tunnistamiseksi käyttää CIR:ä laittoman maahanmuuton estämisen ja torjumisen edistämiseksi tai yleisen järjestyksen ja turvallisuuden ylläpitämiseksi. Kansallinen soveltamisala olisi siten rajoitetumpi kuin poliisi- ja rajayhteentoimivuusasetukset mahdollistaisivat. Soveltamisen ulkopuolelle jätettäisiin mahdollisuus tehdä kysely CIR:ii, kun tarkoituksena olisi korkean turvallisuustason edistäminen unionin vapauden, turvallisuuden ja oikeuden alueella. CIR:n käytön tulisi myös olla välttämätöntä henkilön tunnistamista varten. Oikeus koskisi myös biometristen sormenjälkien ja kasvokuvien käyttöä.

Laittoman maahanmuuton estämisessä ja torjumisessa on olennaista selvittää maahan tulevien ja maassa oleskelevien henkilöiden oikea henkilöllisyys, jos tämä on epäselvä. Tällöin kysely CIR:iin on perusteltu. Samoin yleisen järjestyksen ja turvallisuuden ylläpitämisessä on tärkeää, että toimivaltainen viranomainen pystyy varmistumaan henkilön oikeasta henkilöllisyydestä. Kysely CIR:iin voisi olla tarpeellista, kun toimivaltainen viranomainen ei kykene tunnistamaan henkilöä matkustusasiakirjan tai kyseisen henkilön henkilöllisyyden todistavan muun uskottavan asiakirjan puuttumisen vuoksi tai kun henkilön antamista henkilöllisyystiedoista taikka matkustusasiakirjan aitoudesta tai sen haltijan henkilöllisyydestä on epäilyjä tai jos henkilö ei kykene yhteistyöhön tai kieltäytyy siitä.

Pykälän 2 momentissa säädetään Tullin oikeudesta tehdä kyselyjä CIR:iin henkilön tunnistamiseksi, kun se on sellaisten tavaroiden tai aineiden lainvastaisen maahantuonnin, maasta viennin tai kauttakuljetuksen paljastamiseksi ja torjumiseksi, jotka aiheuttavat vaaraa ihmisille tai ympäristölle. CIR:n käytön tulee myös olla välttämätöntä henkilön tunnistamista varten. Oikeus koskisi myös biometristen sormenjälkien ja kasvokuvien käyttöä. Tullille esitettävät käyttötarkoitukset perustuisivat poliisi- ja rajayhteentoimivuusasetusten 2 artikloiden c kohdissa sanottuun asetusten tavoitteiseen taata turvallisuus jäsenvaltioiden alueella.

Pykälän 3 momentissa viitataan yhteentoimivuusasetusten 20 artiklan 2 ja 3 kohtiin, jossa säädetään tarkemmin menettelyistä, joita toimivaltaisten viranomaisten on noudatettava tehdessään kyselyjä CIR:iin. Poliisin, tullimiehen tai rajavartijan on käynnistettävä henkilön tunnistamista koskeva menettely kyseisen henkilön läsnäollessa. Kyselyä ei saisi tehdä alle 12-vuotiaiden alaikäisten tunnistamiseksi, paitsi jos se on lapsen edun mukaista. Toimivaltainen viranomainen harkitsee, milloin alle 12-vuotiaan alaikäisen edun mukaista on, että hänen henkilöllisyytensä

varmistetaan. Tällainen tilanne voi olla, jos viranomaiselle on esimerkiksi muodostunut käsitys siitä, että lapsi on rikoksen uhri.

Jos CIR:in tehty kysely osoittaa, että CIR:ään on tallennettu kyseistä henkilöä koskevia tietoja, viranomaisella on oikeus päästä katsomaan näitä tietoja. Viranomainen saa siis vain pääsyn CIR:ssä oleviin tietoihin. CIR:ssä on VIS:ään, Eurodaciin, EES:ään, ETIAS:kseen ja ECRIS-TCN:ään tallennetut kolmansien maiden kansalaisia koskevat henkilötiedot sekä biometriikka ja matkustusasiakirjan tiedot. Viranomaisen tehdessä kyselyn CIR:ään, hän saa myös tiedon siitä missä edellä mainitussa tietojärjestelmässä tai tietojärjestelmissä on kyseistä henkilöä koskevia tarkempia tietoja. Näihin tietoihin voi päästä vain kyseisen tietojärjestelmän oikeusperustassa säädetyin edellytyksin.

Jos henkilön biometrisiä tietoja ei voida käyttää tai jos kysely niillä epäonnistuu, kysely voidaan tehdä kyseisen henkilön henkilöllisyystiedoilla yhdessä matkustusasiakirjan tietojen kanssa tai kyseisen henkilön antamilla henkilöllisyystiedoilla.

Pykälän 4 momentin mukaan poliisilla olisi oikeus luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa tehdä kyselyjä CIR:ään tunnistaakseen sellaisen henkilön, joka ei pysty osoittamaan henkilöllisyyttään. Lisäksi poliisilla olisi näissä tilanteissa oikeus tehdä kyselyjä biometrisillä tiedoilla tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi.

Poliisilla on jo tällä hetkellä laaja oikeus selvittää tuntemattoman henkilön tai vainajan henkilöllisyys. Oikeuslääketieteellinen kuolemansyyn selvittäminen kuuluu poliisille. Uhrintunnistustoiminta on osa kuolemansyyn selvittämistä.

Momentissa kyselyoikeutta CIR:ään esitetään vain poliisille, koska se vastaa jo tällä hetkellä henkilöiden tunnistamisesta momentissa tarkoitetuissa tilanteissa eikä tämä kuulu Rajavartiolaitoksen tai Tullin tehtäviin.

8 Voimaantulo

Ehdotetaan, että laki tulee voimaan 1.9.2022.

Komission tämän hetkisen aikataulun mukaan yhteentoimivuuskomponenteista otetaan ensin käyttöön yhteinen BMS vuonna 2022 ja sen jälkeen CIR vuoden 2022 lopulla. Lisäksi tuolloin on käynnissä yhteentoimivuusasetusten artikloiden 20 ja 22 valmistelu, joilla on vaikutusta nyt esitettävään lakiehdotukseen. Kun laki tulisi voimaan syyskuun 2022 alusta, olisi CIR:n tullessa käyttöön hyväksyttynä jo ne viranomaiset, jotka osallistuvat kansalliseen toimeenpanoon.

9 Toimeenpano ja seuranta

Poliisiyhteentoimivuusasetuksen 74 artiklan ja rajayhteentoimivuusasetuksen 78 artiklan mukaan eu-LISA:n tuli toimittaa Euroopan parlamentille ja neuvostolle kertomuksen yhteentoimivuuskomponenttien kehittämisen ja niiden yhdenmukaiseen kansalliseen rajapintaan liittämisen etenemisestä viimeistään 12 päivänä joulukuuta 2019 ja sen jälkeen kuuden kuukauden välein yhteentoimivuuskomponenttien kehittämisvaiheen aikana.

Kun kehittämisvaihe on saatu päätökseen, Euroopan parlamentille ja neuvostolle annetaan kertomus, jossa selitetään yksityiskohtaisesti, miten erityisesti suunnitteluun ja kustannuksiin liittyvät tavoitteet on saavutettu, ja perustellaan mahdolliset poikkeamat tavoitteista. Lisäksi eu-LISA:n tulee toimittaa Euroopan parlamentille, neuvostolle ja komissiolle kertomuksen yhteentoimivuuskomponenttien teknisestä toiminnasta, mukaan lukien niiden turvallisuus, neljän

vuoden kuluttua kunkin yhteentoimivuuskomponentin käyttöönotosta ja sen jälkeen neljän vuoden välein. Komissio laatii vuoden kuluttua eu-LISAn yhteentoimivuuskomponentteja koskevasta kertomuksesta yleisarvioinnin, jossa arvioidaan asetusten soveltamista eri näkökohdista.

Komissio toimittaa myös joka vuosi siihen saakka, kunnes yhteentoimivuuskomponettien täytäntöönpanosta annetut säädökset on hyväksytty, Euroopan parlamentille ja neuvostolle kertomuksen asetusten täysimääräisen täytäntöönpanon valmistelujen tilanteesta. Tässä kertomuksessa on oltava myös yksityiskohtaisia tietoja aiheutuneista kustannuksista sekä tietoja mahdollisista riskeistä, jotka voivat vaikuttaa kokonaiskustannuksiin.

Komissio tarkastelee MID:n vaikutusta syrjimättömyyttä koskevaan oikeuteen kahden vuoden kuluttua MID:n käyttöönotosta.

CIR:n käyttöönoton jälkeen jäsenvaltiot ja Europol laativat vuosittain kertomukset, joissa tarkastellaan, miten tuloksellista pääsy CIR:ään tallennettuihin tietoihin terrorismirikosten tai muiden vakavien rikosten torjumiseksi, havaitsemiseksi tai tutkimiseksi on ollut.

10 Suhde talousarvioesitykseen

Kyseessä on budjettilakiehdotus. Esitys liittyy valtion vuoden 2022 talousarvioesitykseen ja on tarkoitettu käsiteltäväksi sen yhteydessä.

11 Suhde perustuslakiin ja säätämisjärjestys

Poliisi- ja rajayhteentoimivuusasetukset ovat EU:n säädöksiä, jotka ovat kaikilta osiltaan velvoittava ja joita sovelletaan sellaisenaan kaikissa jäsenvaltioissa. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin lainsäädäntö on ensisijaista suhteessa kansallisiin säännöksiin oikeuskäytännössä määriteltyjen edellytysten mukaisesti (PeVL 20/2017 vp, s. 6 ja PeVL 51/2014 vp, s. 2/II). EU-tuomioistuimen vakiintuneen oikeuskäytännön mukaan kansallista sääntelyä ei saa antaa asetuksen soveltamisalalla, ellei asetus nimenomaisesti velvoita tai valtuuta täydentävään kansalliseen sääntelyyn tai muuhun päätöksentekoon (asia 34/73, Variola, tuomio 10.10.1973, asia 50/76, Amsterdam Bulb, tuomio 2.2.1977, 33 kohta).

Ehdotettu sääntely perustuu Suomea sitoviin kansainvälisiin velvoitteisiin. Tällaisen yhteyden perustuslakivaliokunta on todennut sääntelyn hyväksyttävyyttä tukevaksi seikaksi (esimerkiksi PeVL 38/2012 vp, s. 3).

Yhteentoimivuusasetuksilla perustetaan yhteinen biometrinen tunnistuspalvelu, joka luo EU-tason tietojärjestelmiin syötetyistä biometrisistä tunnisteista matemaattisen mallin ja tallentaa sen yhteiseen kantaan. Asetuksilla perustetaan myös yhteinen henkilöllisyystietovaranto ja rinnakkaishenkilöllisyyksien tunnistin, jotka tarvitsevat toimiakseen edellä mainitun biometrisen tunnistuspalvelun.

Toimivaltaisten viranomaisten pääsy henkilöllisyystietovarantoon henkilön tunnistamista varten on asetuksissa jätetty kansallisen liikkumavaran piiriin. Perustuslakivaliokunta on yhteentoimivuusasetuksista antamassaan lausunnossa muistuttanut, että siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä on otettava huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (PeVL 11/2018 vp, ks. myös PeVL 25/2005 vp, PeVL 1/2018 vp).

Asetukset ja niitä täydentävä kansallinen säätely merkitsevät puuttumista yksityiselämän ja henkilötietojen suojaan. Perustuslakivaliokunta on arvioidessaan tällaista sääntelyä yleensä katsonut, että sääntelyä on tarkasteltava perustuslain 10 §:n kannalta. Sen 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa (ks. esim. PeVL 11/2018 vp, PeVL 13/2016 vp).

Yhteentoimivuusasetuksista antamassaan lausunnossa perustuslakivaliokunta katsoi, että EU-tason tietojärjestelmien yhteentoimivuutta säätelevän kehyksen perustamista voidaan pitää pääosin myönteisenä. Perustuslain ja henkilötietojen suojaa koskevien perus- ja ihmisoikeuksien kannalta on perusteltua lisätä eri EU-tason tietojärjestelmien yhteensopivuutta ja -toimivuutta, sillä yhteensopivuudella ja -toimivuudella on mahdollista vähentää eri järjestelmien välisen yhteensopimattomuuden aiheuttamia riskejä oikeusvarmuudelle sekä tietosuojalle ja -turvalle (PeVL 11/2018 vp).

Asetuksissa ja esityksessä ehdotetussa kansallisessa sääntelyssä on kysymys osaksi arkaluonteisia tietoja koskevasta sääntelystä. Perustuslakivaliokunta on korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mukaan ollut syytä suhtautua kielteisesti esimerkiksi laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä (PeVL 14/2009 vp, s. 4/II). Tällaisissa tilanteissa käyttötarkoitussidonnaisuudesta on voitu tällöin tehdä vain täsmällisiä ja vähäisiksi luonnehdittavia poikkeuksia, eikä sääntely ole saanut johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi (PeVL 11/2018 vp, ks. myös esim. PeVL 14/2017 vp, s. 5—6).

Perustuslakivaliokunta on korostanut, että yksityiselämän suojan rajoituksella tulisi olla hyväksyttävä yhteiskunnallinen intressi ja rajoituksen tulisi olla oikeassa suhteessa tavoiteltuun päämäärään. Tämä merkitsee, että rajoitusten tulee olla välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi. Perusoikeuden rajoittaminen on sallittua ainoastaan, jos tavoite ei ole saavutettavissa perusoikeuteen vähemmän puuttuvin keinoin. Rajoitus ei saa mennä pidemmälle kuin on perusteltua ottaen huomioon rajoituksen taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään (PeVM 25/1994 vp, ja esimerkiksi PeVL 56/2014 vp ja PeVL 18/2013 vp).

Perustuslakivaliokunta on myös painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin, kuten yleiseen turvallisuuteen liittyviin intresseihin, jotka voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (PeVL 5/1999 vp, s. 2/II). Lainsäätäjän tulee turvata yksityiselämän ja henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Valiokunta on katsonut, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden. Arvioinnissa on kyse kahden tai useamman perusoikeussäännöksen yhteensovittamisesta ja punninnasta (ks. esim. PeVL 14/2018 vp, s. 8, PeVL 26/2018, s. 4, PeVL 54/2014 vp, s. 2/II ja PeVL 10/2014 vp, s. 4/II).

Esityksessä ehdotetaan yhteentoimivuusasetusten kansallisen liikkumavaran käyttämistä siten, että sääntelyllä mahdollistetaan toimivaltaisten viranomaisten pääsy EU:n yhteiseen henkilöllisyystietovarantoon. Ehdotetut säännökset koskevat arkaluonteisina pidettäviä biometrisia tietoja, joiden käsittely edellyttää siitä aiheutuvien riskien vuoksi täsmällistä ja tarkkarajaista

sääntelyä. Toimivaltaisten viranomaisten joukko esitetään säännöskohtaisissa perusteluissa kuvatuin perustein rajattavaksi poliisiin, Rajavartiolaitokseen ja Tulliin. Pääsy olisi rajattu ainoastaan tilanteisiin, joissa se olisi välttämätöntä lainkohdassa täsmennettyjen tehtävien suorittamiseksi.

Esityksessä ei ehdoteta muutoksia sääntelyyn, joka koskee kansallisiin rekistereihin tallennettujen biometristen tietojen käsittelyedellytyksiä ja luovuttamista EU:n yhteisiin tietojärjestelmiin. Yhteentoimivuusasetuksilla ja täydentävällä kansallisella sääntelyllä ei myöskään muuteta sääntöjä, jotka koskevat viranomaisten pääsyä EU:n yhteisiin tietojärjestelmiin. Näiden järjestelmien käyttöoikeudet perustuvat kunkin tietojärjestelmän oikeusperustaan ja voimassa olevaan kansalliseen sääntelyyn. Rekisteröidyn etuja turvaavat voimassa olevan tietosuojalainsäädännön mukaiset rekisteröidyn oikeudet.

Yhteentoimivuusasetusten tavoitteena on rajatarkastusten tuloksellisuuden ja tehokkuuden parantaminen ulkorajoilla, laittoman maahanmuuton estämisen ja torjumisen edistäminen, korkean turvallisuustason edistäminen unionin vapauden, turvallisuuden ja oikeuden alueella, mukaan lukien yleisen järjestyksen ylläpitäminen ja turvallisuuden takaaminen jäsenvaltioiden alueella, yhteisen viisumipolitiikan täytäntöönpanon parantaminen, kansainvälistä suojelua koskevien hakemusten tutkinnan helpottaminen, terrorismirikosten ja muiden vakavien rikosten torjumisen, havaitsemisen ja tutkimisen edistäminen sekä luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa sellaisten tuntemattomien henkilöiden tunnistamisen, jotka eivät pysty osoittamaan henkilöllisyyttään, tai tunnistamatta jääneiden ihmisten jäännösten tunnistamisen helpottaminen Esityksessä ehdotetun henkilötietojen käsittelyä koskevan sääntelyn on arvioitu olevan välttämätön ja oikeasuhtainen toimenpide ottaen huomioon ehdotusten taustalla olevien tavoitteiden painavuus suhteessa rajoitettavaan perusoikeuteen.

Edellä mainituilla perusteilla lakiehdotus voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Ponsi

Koska yhteentoimivuusasetuksissa on säännöksiä, joita ehdotetaan täydennettäviksi lailla, annetaan eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Lakiehdotus

Laki

Euroopan unionin tietojärjestelmien yhteentoimivuudesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Soveltamisala

Tässä laissa annetaan täydentävät säännökset kehyksen vahvistamisesta rajoja ja viisumipolitiikkaa koskevien EU:n tietojärjestelmien yhteentoimivuudelle ja Euroopan parlamentin ja neuvoston asetusten (EY) N:o 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 ja (EU) 2018/1861 sekä neuvoston päätösten 2004/512/EY ja 2008/633/YOS muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/817 ja kehyksen vahvistamisesta poliisiyhteistyötä ja oikeudellista yhteistyötä sekä turvapaikka- ja muuttoliikeasioita koskevien EU:n tietojärjestelmien yhteentoimivuudelle ja asetusten (EU) 2018/1726, (EU) 2018/1862 ja (EU) 2019/816 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/818, jäljempänä yhteentoimivuusasetukset, soveltamisesta.

2 §

Toimivaltainen viranomainen

Toimivaltaisia viranomaisia, joilla on pääsy yhteentoimivuusasetusten 20 artiklassa säädetyin edellytyksin yhteiseen henkilöllisyystietovarantoon, ovat poliisi, Rajavartiolaitos ja Tulli.

3 §

Pääsy yhteiseen henkilöllisyystietovarantoon

Poliisilla ja Rajavartiolaitoksella on yhteentoimivuusasetusten 20 artiklan 1 kohdassa säädettyjen edellytysten täyttyessä oikeus käyttää yhteistä henkilöllisyystietovarantoa mukaan lukien biometriset sormenjälki- ja kasvokuvatiedot henkilön tunnistamiseksi, kun se on välttämätöntä niille säädetyn laittoman maahanmuuton estämistä ja torjumista koskevan tehtävän tai yleisen järjestyksen ja turvallisuuden ylläpitämistä koskevan tehtävän suorittamiseksi.

Tullilla on yhteentoimivuusasetusten 20 artiklan 1 kohdassa säädettyjen edellytysten täyttyessä oikeus käyttää yhteistä henkilöllisyystietovarantoa mukaan lukien biometriset sormenjälki- ja kasvokuvatiedot henkilön tunnistamiseksi, kun se on välttämätöntä sellaisten tavaroiden tai aineiden lainvastaisen maahantuonnin, maasta viennin tai kauttakuljetuksen paljastamiseksi ja torjumiseksi, jotka aiheuttavat vaaraa ihmisille tai ympäristölle.

Toimivaltaisen viranomaisen on suoritettava kysely yhteisestä henkilötietovarannosta yhteentoimivuusasetusten 20 artiklan 2 ja 3 kohdan mukaisesti.

Sen lisäksi, mitä 1 momentissa säädetään, luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa poliisilla on oikeus tehdä kyselyjä yhteisestä henkilöllisyystietovarannosta sellaisten tuntemattomien henkilöiden tunnistamiseksi, jotka eivät pysty osoittamaan

henkilöllisyyttään tai tehdä kyselyjä biometrisilla tiedoilla tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Helsingissä x.x.20xx

Pääministeri

Sanna Marin

..ministeri Etunimi Sukunimi