EUROOPAN
KOMISSIO

Bryssel 6.4.2016
COM(2016) 205 final

# KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

## Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi

## 1. JOHDANTO

Euroopassa liikutaan paljon. EU:n sisä- ja ulkorajojen yli kulkee päivittäin miljoonia unionin jäsenvaltioiden ja kolmansien maiden kansalaisia. Vuonna 2015 EU:ssa kävi yli 50 miljoonaa kolmannen maan kansalaista. Schengen-alueen ulkorajoilla kirjattiin yli 200 miljoonaa rajanylitystä.

Näiden sääntöjenmukaisten matkustajavirtojen lisäksi unionin ulkorajoilla tapahtui Syyrian konfliktin ja muiden kriisien vuoksi 1,8 miljoonaa sääntöjenvastaista rajanylitystä pelkästään vuonna 2015. Unionin kansalaiset odottavat, että ulkorajoilla tehtävät henkilötarkastukset ovat tehokkaita, niin että muuttoliikettä voidaan niiden avulla hallita tehokkaasti ja edistää siten sisäisen turvallisuuden säilymistä. Pariisissa vuonna 2015 ja Brysselissä maaliskuussa 2016 tehdyt terrori-iskut olivat kuitenkin synkkä muistutus siitä, että Euroopan sisäinen turvallisuus on edelleen uhattuna.

Ne korostivat tarvetta yhdistää voimat rajaturvallisuutta, muuttoliikettä ja sisäistä turvallisuutta koskevien EU:n yhteistyökehysten ja tietojärjestelmien lujittamiseksi kattavalla tavalla. Rajaturvallisuus, lainvalvonta ja muuttoliikkeen hallinta liittyvät dynaamisesti toisiinsa. Unionin kansalaisten tiedetään matkustaneen EU:n ulkopuolelle konfliktialueille terrorismitarkoituksessa. Palattuaan he muodostavat turvallisuusriskin. On myös näyttöä siitä, että terroristit ovat tulleet EU:n alueelle käyttäen hyväkseen sääntöjenvastaisen muuttoliikkeen reittejä ja liikkuneet sitten edelleen Schengen-alueen sisällä paljastumatta.

Euroopan turvallisuus- ja muuttoliikeagendoissa on esitetty suuntaviivat, joiden mukaisesti olisi kehitettävä ja pantava täytäntöön EU:n toimenpiteitä muuttoliikkeen hallintaan ja terrorismin ja järjestäytyneen rikollisuuden torjuntaan liittyvien haasteiden käsittelemiseksi. Tämä tiedonanto perustuu näiden agendojen luomaan synergiaan. Sen tarkoituksena on käynnistää keskustelu siitä, miten olemassa olevien ja tulevien tietojärjestelmien avulla voitaisiin parantaa sekä EU:n ulkorajojen valvontaa että sisäistä turvallisuutta. Tiedonanto täydentää joulukuussa 2015 esitettyä ehdotusta, joka koski Euroopan raja- ja rannikkovartioston perustamista sekä kriisien ehkäisemistä ja interventioita ulkorajoilla.

EU:n tasolla on käytössä useita tietojärjestelmiä, joiden avulla rajavartijat ja poliisiviranomaiset saavat asianmukaisia tietoja henkilöistä. EU:n tietoarkkitehtuurissa on kuitenkin parantamisen varaa. Tässä tiedonannossa esitetään eräitä vaihtoehtoja, joiden avulla nykyisiä tietojärjestelmiä voitaisiin hyödyntää mahdollisimman tehokkaasti ja tarvittaessa kehittää uusia ja täydentäviä toimia puutteiden korjaamiseksi. Lisäksi siinä korostetaan, että pitkällä aikavälillä on tarpeen parantaa tietojärjestelmien yhteentoimivuutta, kuten myös Eurooppa-neuvosto ja Euroopan unionin neuvosto ovat todenneet.[1] Tiedonannossa esitetään myös ideoita siitä, miten tietojärjestelmiä voitaisiin kehittää jatkossa niin, että rajavartijat, tulliviranomaiset, poliisit ja oikeusviranomaiset saavat tarvittavat tiedot käyttöönsä.

Myöhemmin mahdollisesti esitettävät aloitteet laaditaan paremman sääntelyn periaatteita noudattaen julkisen kuulemisen ja vaikutustenarvioinnin pohjalta perusoikeuksia ja erityisesti henkilötietojen suojaa kunnioittaen.

[1] Brysselissä 17. ja 18. joulukuuta 2015 kokoontuneen Eurooppa-neuvoston päätelmät; EU:n oikeus- ja sisäasiainministerien ja EU:n toimielinten edustajien yhteinen lausuma Brysselissä 22. maaliskuuta 2016 tehdyistä terrori-iskuista (24.3.2016); Euroopan unionin neuvoston ja neuvostossa kokoontuneiden jäsenvaltioiden päätelmät terrorismin torjunnasta (20.11.2015).

## 2. HAASTEET

Koska Schengen-alueella ei ole sisärajoja, henkilöiden liikkuminen yli ulkorajojen edellyttää vahvaa ja luotettavaa valvontaa. Vain tällä tavoin voidaan varmistaa sisäisen turvallisuuden korkea taso ja ihmisten vapaa liikkuvuus Schengen-alueella. Toisaalta sisärajojen puuttuminen tarkoittaa sitä, että myös jäsenvaltioiden lainvalvontaviranomaisilla on oltava pääsy henkilöitä koskeviin tietoihin. EU:n tasolla on käytössä lukuisia tietojärjestelmiä ja tietokantoja, joiden avulla rajavartijat, poliisit ja muut viranomaiset saavat tarvittavat tiedot henkilöistä omia tarpeitaan varten.[2]

Tietojärjestelmissä on kuitenkin puutteita, jotka vaikeuttavat näiden kansallisten viranomaisten työtä. Siksi Euroopan turvallisuusagendassa korostetaan tietojenvaihdon parantamisen merkitystä. Suurimpia puutteita ovat a) nykyisten tietojärjestelmien puutteellinen toiminta, b) EU:n tietoarkkitehtuurin aukot, c) eri tavoin hallinnoiduista tietojärjestelmistä muodostuvan kokonaisuuden monimutkaisuus, ja d) rajavalvontaa ja -turvallisuutta koskevan tietoarkkitehtuurin hajanaisuus.

Rajaturvallisuuteen ja sisäiseen turvallisuuteen liittyvät EU:n nykyiset tietojärjestelmät kattavat monenlaisia toimintoja. **Nykyisten järjestelmien toiminnassa** on kuitenkin **puutteita**. Eri matkustajaryhmiin sovellettavien rajavalvontamenettelyjen tarkastelu osoittaa selvästi, että ongelmia on sekä eräissä menettelyissä että niiden toteuttamiseen käytettävissä tietojärjestelmissä. Parannettavaa on myös nykyisten lainvalvontavälineiden toiminnassa. Tätä varten on pohdittava, miten nykyisiä tietojärjestelmiä voitaisiin kehittää (5 jakso).

Toisaalta myös **EU:n tietoarkkitehtuurissa on aukkoja**. Ongelmia tuottaa edelleen rajatarkastusten tekeminen tietyille matkustajaryhmille, kuten pitkäaikaisella viisumilla matkustaville kolmansien maiden kansalaisille. Myöskään niistä kolmansien maiden kansalaisista, joilta ei vaadita viisumia, ei ole saatavissa riittävästi tietoja ennen kuin he saapuvat rajalle. Olisikin pohdittava, olisiko näiden ongelmien korjaamiseksi tarpeen kehittää uusia tietojärjestelmiä (6 jakso).

Rajavartijat ja varsinkin poliisit joutuvat tekemisiin EU:n tasolla **monin eri tavoin hallinnoiduista tietojärjestelmistä muodostuvan monimutkaisen kokonaisuuden** kanssa. Se aiheuttaa käytännön ongelmia, jotka liittyvät muun muassa siihen, mitä tietokantoja olisi tarkistettava missäkin tilanteessa. Lisäksi kaikki jäsenvaltiot eivät ole mukana kaikissa nykyisissä järjestelmissä.[3] Pääsyä EU:n tason tietojärjestelmiin voitaisiin helpottaa ottamalla kansallisella tasolla käyttöön yksi ainoa hakuliittymä, jossa otettaisiin huomioon eri tarkoituksia varten myönnetyt käyttöoikeudet (7.1 jakso).

Rajaturvallisuuteen ja sisäiseen turvallisuuteen liittyvä EU:n tietoarkkitehtuuri on **hajanainen**. Tämä johtuu siitä, että järjestelmien kehittämiseen liittyvät institutionaaliset, oikeudelliset ja poliittiset taustat ovat erilaisia. Tiedot tallennetaan erikseen eri järjestelmiin, jotka eivät yleensä ole yhteydessä toisiinsa. Tietokannat ovat keskenään yhteensopimattomia, ja viranomaisten oikeudet käyttää niitä vaihtelevat. Tämä saattaa johtaa varsinkin lainvalvontaviranomaisten kannalta katvealueiden

[2] Ks. 4 jakso, jossa on yhteenveto rajaturvallisuutta ja sisäistä turvallisuutta koskevista tietojärjestelmistä, ja liite 2, jossa esitetään yksityiskohtaisempi luettelo niistä.

[3] Tämä johtuu erityisehdoista, jotka on määritelty Tanskan osalta pöytäkirjassa N:o 22, Yhdistyneen kuningaskunnan ja Irlannin osalta pöytäkirjoissa N:o 21 ja 36 sekä näitä jäsenvaltioita koskevissa liittymissopimuksissa.

muodostumiseen, koska tiedonsirpaleiden välisiä yhteyksiä voi olla hyvin vaikea havaita. Sen vuoksi on välttämätöntä pyrkiä kiireellisesti luomaan yhdennettyjä ratkaisuja rajaturvallisuutta ja sisäistä turvallisuutta koskevien tietojen saatavuuden parantamiseksi perusoikeuksia täysimääräisesti kunnioittaen. Tätä varten olisi käynnistettävä prosessi nykyisten tietojärjestelmien yhteentoimivuuden parantamiseksi (7 jakso).

## 3. PERUSOIKEUDET

Perusoikeuksien ja tietosuojasääntöjen täysimääräinen noudattaminen on olennainen edellytys kaikkiin edellä kuvattuihin haasteisiin puuttumisessa.

Perusoikeuksien noudattaminen edellyttää, että teknologia ja tietojärjestelmät on suunniteltu hyvin ja että niitä käytetään asianmukaisella tavalla. Näin ne voivat olla viranomaisille apuna kansalaisten perusoikeuksien suojelemisessa. Biometrisen tunnistamisen avulla voidaan vähentää väärän henkilöllisyyden käyttöön sekä syrjintään ja rotuprofilointiin liittyviä riskejä. Siitä on apua myös lasten suojeluun liittyvien riskien vähentämisessä eli kun on kyse esimerkiksi kadonneista tai ihmiskaupan uhreiksi joutuneista lapsista, kunhan sen soveltamisessa noudatetaan perusoikeuksiin liittyviä takeita ja suojatoimia. Biometrisen tunnistamisen avulla voidaan vähentää myös aiheettomien kiinniottojen ja pidätysten riskiä. Lisäksi se voi parantaa Schengen-alueella asuvien kansalaisten turvallisuutta, koska siitä on apua terrorismin ja vakavan rikollisuuden torjunnassa.

Laaja-alaisiin tietojärjestelmiin liittyy myös potentiaalisia yksityisyydensuojaa koskevia riskejä, joihin on varauduttava ja puututtava asianmukaisella tavalla. Henkilötietojen kerääminen ja käyttö näissä järjestelmissä vaikuttaa Euroopan unionin perusoikeuskirjassa vahvistettuun yksityisyyttä ja henkilötietojen suojaa koskevaan oikeuteen. Kaikkien järjestelmien yhteydessä on noudatettava tietosuojaperiaatteita sekä tietojen tarpeellisuutta, oikeasuhteisuutta, käyttötarkoituksen rajoittamista ja laatua koskevia vaatimuksia. Käytössä on oltava takeet, joiden avulla varmistetaan rekisteröityjen oikeudet suhteessa yksityiselämän ja henkilötietojen suojaan. Tietoja olisi säilytettävä vain niin kauan kuin se on tarpeen sitä tarkoitusta varten, johon ne on kerätty. Käytössä on myös oltava mekanismit, joiden avulla varmistetaan asianmukainen riskienhallinta ja rekisteröityjen oikeuksien tehokas suojelu.

Lainsäätäjät pääsivät joulukuussa 2015 poliittiseen yhteisymmärrykseen tietosuojauudistuksesta. Kun yleinen tietosuoja-asetus ja poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi on hyväksytty[4], niitä ryhdytään soveltamaan vuonna 2018, ja ne muodostavat henkilötietojen käsittelylle yhdenmukaiset puitteet.

Käyttötarkoituksen rajoittamisen periaate on perusoikeuskirjassa vahvistettu keskeinen tietosuojaperiaate. Koska EU:n tason tietojärjestelmät on kehitetty eri toimielinten puitteissa ja erilaisissa oikeudellisissa ja toimintaympäristöissä, käyttötarkoituksen rajoittamisen periaate on pantu täytäntöön tiedonhallinnan osastoivan rakenteen[5] avulla. Tämä on yksi syy rajaturvallisuuden ja sisäisen turvallisuuden alalla käytettävän EU:n tietoarkkitehtuurin hajanaisuuteen. Kun EU:ssa otetaan käyttöön henkilötietojen suojaa koskeva uusi kattava kehys, käyttötarkoituksen rajoittamisen periaate voidaan teknologian ja tietoturvallisuuden huomattavan kehityksen ansiosta toteuttaa nykyistä helpommin tallennettuihin tietoihin pääsyn ja niiden käytön tasolla perusoikeuskirjaa ja Euroopan

[4] Ks. http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[5] COM(2010) 385 final.

unionin tuomioistuimen viimeaikaista oikeuskäytäntöä täysimääräisesti noudattaen. Tarvittava käyttötarkoituksen rajoittaminen voidaan varmistaa yhdennetyissä tiedonhallintajärjestelmissä erilaisten suojatoimien avulla, kuten jakamalla järjestelmän tiedot eri osastoihin ja eriyttämällä tietoihin pääsyä ja niiden käyttöä koskevat säännöt tietoluokkien ja käyttäjäryhmien mukaan. Tämä luo edellytykset tietojärjestelmien yhteentoimivuudelle. Sitä varten tarvitaan tietoihin pääsyä ja niiden käyttöä koskevat tiukat säännöt, jotka eivät saa heikentää käyttötarkoituksen rajoittamisen periaatetta nykyisestään.

Sisäänrakennettu ja oletusarvoinen tietosuoja ovat nyt EU:n tietosuojasääntöjen perusperiaatteita. Komissio pyrkii noudattamaan niitä myös kehittäessään tietotekniikan käyttöön perustuvia uusia välineitä. Tämä tarkoittaa, että henkilötietojen suojelu on otettava huomioon jo ehdotetun välineen teknologisessa perustassa, että tietojen käsittely on rajoitettava siihen, mikä on halutun tavoitteen saavuttamiseksi välttämätöntä, ja että pääsy tietoihin on annettava vain niille yksiköille, jotka tarvitsevat niitä tehtäviensä hoitamiseksi.[6]

Pyrkiessään korjaamaan rajaturvallisuutta ja sisäistä turvallisuutta koskevan EU:n tietoarkkitehtuurin aukkoja ja puutteita komissio käyttää ohjenuorana perusoikeuskirjan vaatimuksia ja etenkin tietosuojauudistukseen perustuvia uusia välineitä. Näin varmistetaan, että näillä aloilla käytettävien tietojärjestelmien kehittäminen edelleen tapahtuu tiukimpien tietosuojanormien mukaisesti ja että siinä noudatetaan ja edistetään perusoikeuskirjassa vahvistettuja perusoikeuksia.

## 4. RAJATURVALLISUUDEN JA SISÄISEN TURVALLISUUDEN ALALLA KÄYTETTÄVÄT TIETOJÄRJESTELMÄT[7]

Rajaturvallisuuden ja sisäisen turvallisuuden alalla käytettävillä EU:n tietojärjestelmillä on kullakin omat tavoitteensa, käyttötarkoituksensa, oikeusperustansa[8], käyttäjäryhmänsä ja institutionaalinen toimintaympäristönsä. Yhdessä nämä tärkeät tietokannat muodostavat monimutkaisen kokonaisuuden.

Kolme tärkeintä EU:n perustamaa **keskitettyä tietojärjestelmää** ovat i) Schengenin tietojärjestelmä (SIS), jossa on mahdollista tehdä monenlaisia kuulutuksia henkilöistä ja esineistä, ii) viisumitietojärjestelmä (VIS), johon kootaan tiedot lyhytaikaista oleskelua varten myönnetyistä viisumeista, ja iii) Eurodac-järjestelmä, johon tallennetaan turvapaikanhakijoiden ja unionin ulkorajat sääntöjenvastaisesti ylittäneiden kolmansien maiden kansalaisten sormenjälkitiedot. Nämä järjestelmät täydentävät toisiaan ja koskevat SIS-järjestelmää lukuun ottamatta ensisijaisesti kolmansien maiden kansalaisia. Järjestelmistä on apua kansallisille viranomaisille myös rikollisuuden ja terrorismin torjunnassa.[9] Tämä pätee erityisesti SIS-järjestelmään, joka on nykyisistä järjestelmistä

---

[6] Sisäänrakennetun yksityisyydensuojan periaatetta käsitellään perusteellisesti Euroopan tietosuojavaltuutetun lausunnossa luottamuksen lisäämisestä tietoyhteiskuntaa kohtaan tietosuojaa ja yksityisyyden suojaa parantamalla. Euroopan tietosuojavaltuutettu, 18.3.2010.

[7] Liitteessä 2 on luettelo rajaturvallisuuden ja lainvalvonnan alalla käytettävistä tietojärjestelmistä.

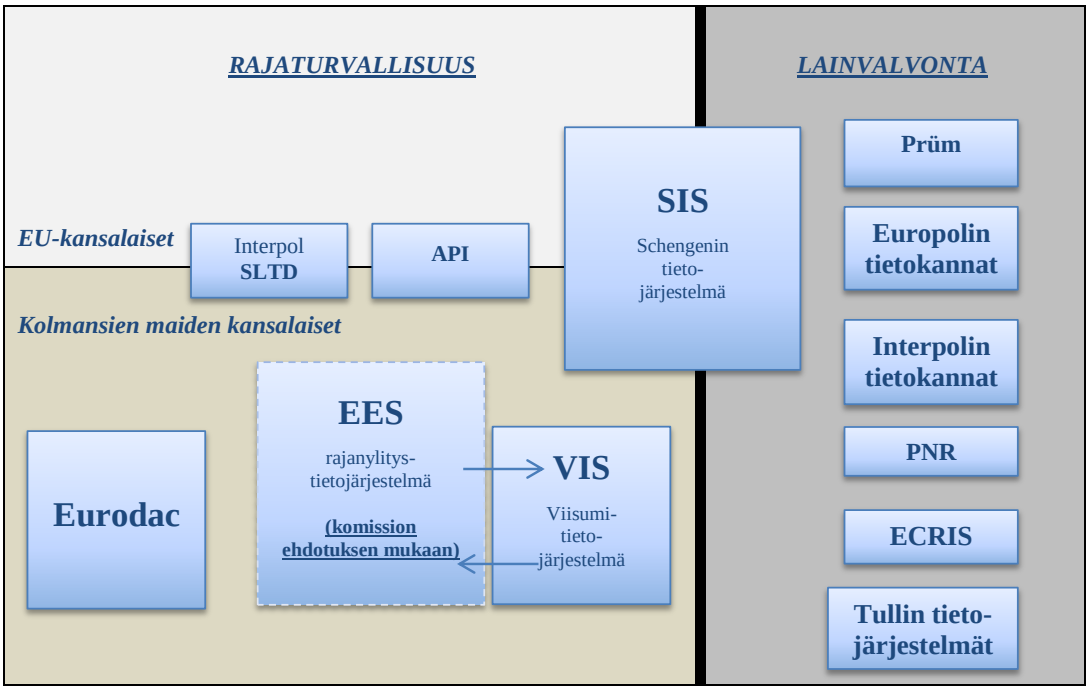
[8] Ellei Tanskaa koskevassa pöytäkirjassa N:o 22 ja Yhdistynyttä kuningaskuntaa ja Irlantia koskevissa pöytäkirjoissa N:o 21 ja 36 vahvistetuista erityisehdoista muuta johdu.

[9] Lainvalvontaviranomaisilla on rajoitettu pääsy VIS- ja Eurodac-järjestelmiin, koska lainvalvonta on näiden järjestelmien toissijainen tavoite. VIS-järjestelmässä jäsenvaltioiden on nimettävä vastuuviranomainen, joka valvoo järjestelmän käyttöä lainvalvontatarkoituksiin. Poliisin on myös esitettävä näyttöä siitä, että pääsy tietoihin on tarpeen rikostutkintaa varten. Eurodac-järjestelmän osalta tutkinnasta vastaavan viranomaisen on tehtävä ensin haut kansalliseen AFIS-, Prüm- ja viisumitietojärjestelmään ennen kuin pääsy Eurodac-järjestelmään voidaan myöntää.

laajimmin käytetty. Tietojen jakaminen näissä järjestelmissä tapahtuu erityisessä suojatussa viestintäinfrastruktuurissa nimeltä sTESTA[10].

Komissio ehdottaa, että näiden järjestelmien lisäksi perustettaisiin neljäs rajaturvallisuutta koskeva keskitetty tietojärjestelmä, **rajanylitystietojärjestelmä** (Entry-Exit System, EES)[11]. Tämä niin ikään kolmansien maiden kansalaisia koskeva järjestelmä voitaisiin ottaa käyttöön vuoteen 2020 mennessä.

***Kaavio 1*** *Yleiskatsaus tärkeimpiin rajaturvallisuutta ja lainvalvontaa koskeviin tietojärjestelmiin:*




Muita rajaturvallisuuden alalla käytettäviä välineitä ovat varastettuja ja kadonneita matkustusasiakirjoja koskeva Interpolin tietokanta (Stolen and Lost Travel Documents, SLTD) sekä matkustajien ennakkotietoja koskeva tietokanta (Advance Passanger Information, API), johon kootaan tiedot matkustajista ennen kuin nämä nousevat EU:n alueelle saapuvalle lennolle. Nämä välineet koskevat sekä unionin että kolmansien maiden kansalaisia.

Lisäksi EU:ssa on kehitetty erityisesti lainvalvontaa, rikostutkintaa ja oikeudellista yhteistyötä varten **hajautettuja tietojenvaihtovälineitä**. Näitä ovat 1) Prüm-puitteet DNA-tietojen, sormenjälkitietojen ja ajoneuvojen rekisteröintitietojen vaihtoa varten ja 2) eurooppalainen rikosrekisteritietojärjestelmä ECRIS, jossa vaihdetaan kansallisia rikosrekisteritietoja. ECRISin avulla voidaan vaihtaa suojatussa verkossa tietoja tietylle henkilölle Euroopan unionin rikostuomioistuimissa aiemmin annetuista tuomioista. Tietopyynnöt perustuvat pääasiassa alfanumeerisiin henkilötietoihin, mutta myös biometrisiä tietoja voidaan vaihtaa.

EU:n rikostietojen keskuksena **Europol** tukee kansallisten poliisiviranomaisten keskinäistä tietojenvaihtoa. Europolin tietojärjestelmä (EIS) muodostaa keskitetyn rikostietokannan, johon jäsenvaltiot voivat tallentaa vakavaa rikollisuutta ja terrorismia koskevia tietoja ja jossa ne voivat tehdä niitä koskevia hakuja. Europolin kansalliset yhteyspisteet laativat

[10] Sen tilalle tulee pian TESTA-NG.
[11] COM(2016) 194 final.

aihealueisiin perustuvia analyysitietokantoja, joissa on tietoa jäsenvaltioissa vireillä olevista operaatioista. Europolin suojatun tiedonvaihtoverkkosovelluksen (Secure Information Exchange Network Application, SIENA) avulla jäsenvaltiot voivat vaihtaa tietoja nopeasti, turvallisesti ja helposti sekä keskenään että Europolin tai sellaisten kolmansien osapuolten kanssa, jotka ovat tehneet yhteistyösopimuksen Europolin kanssa. Lisäksi SIENAssa painotetaan voimakkaasti yhteentoimivuutta Europolin muiden järjestelmien kanssa, jotta tietoja voidaan vaihtaa suoraan esimerkiksi kansallisten yhteyspisteiden kanssa. Näin Europolin tietokantoihin voidaan syöttää tietoja, joita jäsenvaltiot ovat vaihtaneet keskenään. Tästä syystä jäsenvaltioiden olisi käytettävä ensisijaisesti SIENAa, kun ne vaihtavat lainvalvontatietoja EU:n sisällä.

Edellä mainittujen lisäksi jäsenvaltioissa on tarkoitus kehittää tietojärjestelmiä **matkustajarekisteritietojen** (Passenger Name Record, PNR) käsittelyä varten.[12] Matkustajarekisteritiedot koostuvat matkan varauksen ja lähtöselvityksen yhteydessä annettavista tiedoista.

Myös **tulliviranomaiset** ovat keskeinen toimija ulkorajoilla tehtävässä eri virastojen yhteistyössä. Niiden käytössä on erilaisia järjestelmiä[13] ja tietokantoja, jotka sisältävät tietoja tavaroiden liikkumisesta, talouden toimijoiden henkilöllisyydestä ja erilaisista riskeistä ja jotka voivat siksi olla avuksi sisäisen turvallisuuden varmistamisessa. Myös näillä järjestelmillä on oma valvottu, käyttöoikeuksiltaan rajattu ja suojattu infrastruktuuri, käyttökelpoiseksi osoittautunut yhteinen tietoliikenneverkko (Common Communication Network, CCN). Olisikin tutkittava perusteellisemmin mahdollisuuksia kehittää synergiaetuja ja yhdenmukaisuutta tietojärjestelmien ja niiden toimintainfrastruktuurien välillä EU:n rajaturvallisuuden ja tullioperaatioiden alalla.

## 5. NYKYISTEN TIETOJÄRJESTELMIEN PARANTAMINEN

Rajaturvallisuuteen ja sisäiseen turvallisuuteen liittyvät EU:n nykyiset tietojärjestelmät kattavat monenlaisia toimintoja. Järjestelmissä on kuitenkin vielä **puutteita**, jotka on korjattava, jotta ne toimisivat parhaalla mahdollisella tavalla.

*Schengenin tietojärjestelmä (SIS)*

Rajatarkastukset **Schengenin tietojärjestelmässä** (SIS) tehdään nykyään alfanumeerisiin tietoihin (nimi ja syntymäaika) perustuvien hakujen pohjalta. Sormenjälkitietojen avulla voidaan ainoastaan tarkistaa ja varmentaa henkilöllisyys sen jälkeen, kun se on ensin selvitetty nimen avulla. Tämän turvallisuusvajeen takia kuulutuksen kohteena olevat henkilöt voivat väärennettyjen asiakirjojen avulla välttää osuman SIS-järjestelmässä.

Tämä kriittinen heikkous on tarkoitus korjata lisäämällä SIS-järjestelmään sormenjälkihaku **sormenjälkien automaattisen tunnistusjärjestelmän (AFIS)** pohjalta, kuten voimassa olevassa lainsäädännössä[14] todetaan. AFIS-toiminto on tarkoitus saada

[12] Ks. 6.2 jakso.

[13] Tullin tietojärjestelmiin kuuluvat kaikki järjestelmät, joiden kehittäminen perustuu yhteisön tullikoodeksiin (asetus 2913/92), tulevaan unionin tullikoodeksiin (asetus 952/2013) ja paperitonta tullin ja kaupan toimintaympäristöä koskevaan päätökseen (päätös 70/2008/EY), sekä tullitietojärjestelmä, joka perustuu vuonna 1995 tehtyyn yleissopimukseen tietotekniikan käytöstä tullialalla. Tullin tietojärjestelmien tarkoituksena on edistää tullialaan liittyvien rikosten torjuntaa Euroopan tulliviranomaisten keskinäistä yhteistyötä helpottamalla.

[14] Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, annettu 20 päivänä joulukuuta 2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, 22 artiklan c alakohta (EUVL L 381, 28.12.2006, s. 4) ja neuvoston päätös 2007/533/YOS, tehty 12

käyttöön vuoden 2017 puoliväliin mennessä.[15] Kun AFIS on valmis, myös Europolilla on pääsy siihen, joten se täydentää Europolin rikostutkinta- ja terrorismintorjuntajärjestelmiä sekä Prüm-puitteiden mukaista sormenjälkitietojen vaihtoa. Komissio ja eu-LISA selvittävät, olisiko AFIS-järjestelmää mahdollista käyttää tällaisiin laajempiin tarkoituksiin.

Komissio tutkii parhaillaan tehtävien arviointien ja teknisten selvitysten avulla **SIS-järjestelmään mahdollisesti lisättäviä toimintoja** voidakseen tarvittaessa tehdä ehdotuksia SIS-järjestelmän oikeusperustan tarkistamiseksi. Tutkittavana ovat muun muassa seuraavat ehdotukset:

- SIS-kuulutuksen tekeminen sääntöjenvastaisesti maahan tulleista henkilöistä, joista on tehty palautuspäätös
- kasvokuvan käyttö biometrisessä tunnistuksessa sormenjälkitietojen ohella
- automaattisen ilmoituksen toimittaminen tarkastuksen tuloksena saadusta osumasta
- salaista tarkkailua tai erityistarkastusta koskevan kuulutuksen perusteella saatuun osumaan liittyvien tietojen tallentaminen SIS-järjestelmän keskustietokantaan
- uuden kuulutusluokan perustaminen ”etsintäkuulutetuille tuntemattomille henkilöille”, joista voi olla saatavilla rikosteknisiä tietoja kansallisissa tietokannoissa (esim. rikospaikalle jäänyt latentti sormenjälki).[16]

Komissio myöntää myös jatkossa EU-rahoitusta kehityshankkeille, joiden avulla mahdollistetaan hakujen tekeminen samanaikaisesti SIS-järjestelmässä ja EU:n tietojärjestelmiä täydentävissä Interpolin tietokannoissa, jotka koskevat varastettuja ja kadonneita matkustusasiakirjoja (SLTD), etsintäkuulutettuja rikollisia, ajoneuvoja sekä laittomia aseita (iARMS).[17]

*Varastettuja ja kadonneita matkustusasiakirjoja koskeva Interpolin tietokanta (SLTD)*

Tehokkaan rajaturvallisuuden kannalta on olennaisen tärkeää, että kaikkien kolmansien maiden kansalaisten ja EU:n kansalaisten matkustusasiakirjat tarkistetaan varastettuja ja kadonneita matkustusasiakirjoja koskevan **SLTD-tietokannan** avulla. Myös lainvalvontaviranomaisten pitäisi käyttää SLTD-tietokantaa Schengen-alueella tehtävissä hauissa. Pariisissa 13. marraskuuta 2015 tehtyjen terrori-iskujen seurauksena neuvosto vaati, että kaikille ulkorajojen ylityspaikoille on saatava tietoliikenneyhteys tarvittaviin Interpolin tietokantoihin ja että kaikki matkustusasiakirjat on tarkastettava automaattisesti maaliskuuhun 2016 mennessä.[18] Kaikkien jäsenvaltioiden olisi otettava käyttöön tarvittavat tietoliikenneyhteydet ja järjestelmät, joiden avulla tiedot varastetuista

---

päivänä kesäkuuta 2007, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, 22 artiklan c alakohta (EUVL L 2015, 7.8.2007, s. 63).

15 Komissio on esittänyt Euroopan parlamentille ja neuvostolle maaliskuussa 2016 kertomuksen, jossa tarkastellaan sellaisen teknologian saatavuutta ja käyttökelpoisuutta, jonka avulla henkilö voitaisiin tunnistaa toisen sukupolven Schengenin tietojärjestelmässä (SIS II) olevien sormenjälkitietojen perusteella.

16 Uuden kuulutusluokan perustamista harkittaessa otetaan huomioon täydentävyys ja päällekkäisyyksien välttäminen nykyisten Prüm-puitteiden kanssa, koska niiden perusteella on jo mahdollista tehdä sormenjälkihakuja EU:n jäsenvaltioiden eri tietokannoissa.

17 Interpolin kehittämät hakuvälineet, kuten Fixed Interpol Networked Database (FIND) ja Mobile Interpol Networked Database (MIND), on tarkoitettu helpottamaan hakujen tekemistä samanaikaisesti Interpolin järjestelmissä ja SIS-järjestelmässä.

18 Euroopan unionin neuvoston ja neuvostossa kokoontuneiden jäsenvaltioiden päätelmät terrorismin torjunnasta, 20.11.2015.

ja kadonneista matkustusasiakirjoista voidaan päivittää SLTD-tietokannassa automaattisesti.

*Matkustajien ennakkotiedot (API)*

Jäsenvaltioiden olisi nykyisten parhaiden käytäntöjen mukaisesti myös parannettava **matkustajien ennakkotiedoista** (API) saatavaa lisäarvoa ottamalla käyttöön näiden tietojen automaattinen ristiintarkistus SIS-järjestelmän ja SLTD-tietokannan kanssa. Komissio arvioi, olisiko ennakkotietojen käsittelyä koskevaa oikeusperustaa tarkistettava, jotta voitaisiin varmistaa niiden laajempi käyttö ja velvoittaa jäsenvaltiot vaatimaan nämä tiedot ja käyttämään niitä kaikilla sekä saapuvilla että lähtevillä lennoilla. Tämä on erityisen tärkeää tulevan matkustajarekisteridirektiivin täytäntöönpanon yhteydessä, koska käyttämällä PNR- ja API-tietoja yhdessä voidaan edelleen parantaa PNR-tietojen tuloksellisuutta terrorismin ja vakavan rikollisuuden torjunnassa.[19]

*Viisumitietojärjestelmä (VIS)*

Komissio suorittaa parhaillaan **viisumitietojärjestelmän** (VIS) kokonaisarviointia, jonka on tarkoitus valmistua vuoden 2016 aikana. Siinä tarkastellaan muun muassa sitä, miten viisumitietojärjestelmää käytetään ulkorajoilla ja jäsenvaltioiden alueella tehtävissä tarkastuksissa ja miten se edistää henkilöllisyys- ja viisumipetosten torjuntaa. Tältä pohjalta komissio selvittää, voitaisiinko viisumitietojärjestelmän toimintoja tehostaa esimerkiksi

- parantamalla kasvokuvien laatua, jotta niitä voitaisiin käyttää biometrisessä tunnistuksessa
- käyttämällä viisuminhakijoiden biometrisiä tietoja hakuperusteena SIS-järjestelmää varten kehitettävässä sormenjälkien automaattisessa tunnistusjärjestelmässä (AFIS)
- alentamalla sormenjälkitietojen ottamisen ikäraja 6–12-vuotiaisiin lapsiin siten, että samalla säädettäisiin vahvoista perusoikeustakeista ja suojelutoimista[20]
- helpottamalla hakujen tekemistä Interpolin SLTD-tietokannassa viisumihakemuksen käsittelyä varten.

Viisumitietojärjestelmää on mahdollista käyttää **lainvalvontatarkoituksiin** jo nykyisen oikeuskehyksen perusteella, mutta jäsenvaltiot hyödyntävät tätä mahdollisuutta vaihtelevasti. Ne ovat raportoineet tähän liittyvistä käytännön ongelmista, jotka ovat vaikeuttaneet lainvalvontaviranomaisten pääsyä järjestelmään. Myös Eurodac-järjestelmään pääsy lainvalvontatarkoituksissa on toteutunut toistaiseksi hyvin rajoitetusti. Komissio selvittää, olisiko syytä tarkistaa oikeudellista kehystä, joka koskee lainvalvontatarkoituksissa tapahtuvaa pääsyä viisumitietojärjestelmään ja Eurodac-järjestelmään.

*EURODAC*

Kuten tiedonannossa *Euroopan yhteisen turvapaikkajärjestelmän uudistaminen ja laillisten maahanpääsyväylien kehittäminen*[21] todetaan, komissio aikoo esittää ehdotuksen **Eurodac-järjestelmän** uudistamisesta, jotta sen toimintoja voitaisiin tehostaa sääntöjenvastaisen muuttoliikkeen ja palauttamisen tarpeita varten. Tarkoituksena on korjata puute, jonka vuoksi nykyään ei ole mahdollista seurata EU:n alueelle sääntöjenvastaisesti tulleiden henkilöiden edelleen liikkumista jäsenvaltiosta

[19] Ks. 6.2 jakso, jossa esitetään lisätietoja ehdotetusta matkustajarekisteridirektiivistä.

[20] Idea on todettu teknisesti toteuttamiskelpoiseksi YTK:n selvityksessä *Fingerprint Recognition for children;* EUR 26193 EN; ISBN 978-92-79-33390-3Children, 2013.

[21] COM(2016) 197 final.

toiseen. Lisäksi ehdotuksessa pyritään tehostamaan palauttamis- ja takaisinottomenettelyjä ottamalla käyttöön keinot selvittää EU:n alueelle sääntöjenvastaisesti tulleiden henkilöllisyys ja hankkia heille palauttamista varten tarvittavat asiakirjat. Tätä varten ehdotuksessa käsitellään myös Eurodaciin sisältyvien tietojen vaihtoa kolmansien maiden kanssa, tarvittavat tietosuojatakeet huomioon ottaen.

*Europol*

EU on myöntänyt **Europolille** pääsyn tärkeimpiin keskustietokantoihin, mutta virasto ei ole vielä hyödyntänyt tätä mahdollisuutta täysimääräisesti. Europolilla on oikeus päästä SIS-järjestelmään ja tehdä siellä suoria hakuja tietoihin, jotka koskevat kiinniottoa, salaista tarkkailua ja erityistarkastusta sekä takavarikoitavia esineitä. Tähän mennessä Europol on tehnyt SIS-järjestelmässä vain suhteellisen vähän hakuja. Viisumitietojärjestelmää Europolilla on ollut oikeus käyttää syyskuusta 2013 alkaen. Eurodac-järjestelmän oikeusperusta taas on mahdollistanut Europolin pääsyn tietoihin heinäkuusta 2015 alkaen. Europolin olisi kiirehdittävä toimia yhteyden luomiseksi viisumitietojärjestelmään ja Eurodaciin. Komissio pohtii, olisiko pääsy tietojärjestelmiin annettava myös muille sisäasioiden alalla toimiville EU:n virastoille, kuten tulevalle Euroopan raja- ja rannikkovartiostolle.

*Prüm-puitteet*

**Prüm-puitteita** ei tätä nykyä hyödynnetä niin hyvin kuin olisi mahdollista. Tämä johtuu siitä, että kaikki jäsenvaltiot eivät ole noudattaneet oikeudellisia velvoitteitaan verkoston yhdentämiseksi omiin järjestelmiinsä. Jäsenvaltiot ovat saaneet Prüm-puitteiden täytäntöönpanoa varten huomattavan määrän taloudellista ja teknistä tukea, joten niiden olisi pitänyt saada työ jo loppuun. Komissio käyttää sille annettuja valtuuksia varmistaakseen, että jäsenvaltiot noudattavat niille kuuluvia oikeudellisia velvoitteita täysimääräisesti. Se on aloittanut asianomaisten jäsenvaltioiden kanssa tätä aihetta koskevan jäsennellyn vuoropuhelun (EU Pilot) tammikuussa 2016. Jos jäsenvaltioiden vastaukset eivät ole tyydyttäviä, komissio ei epäröi käynnistää rikkomusmenettelyjä.

*Eurooppalainen rikosrekisteritietojärjestelmä (ECRIS)*

Eurooppalainen rikosrekisteritietojärjestelmä **ECRIS** mahdollistaa aiempia tuomioita koskevan tietojenvaihdon myös kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden osalta, mutta se ei ole tällä hetkellä kovin tehokasta. Komissio antoikin tammikuussa 2016 säädösehdotuksen[22] tämän puutteen korjaamiseksi. Komissio ehdottaa siinä, että kansalliset viranomaiset voisivat tehdä kolmansien maiden kansalaisia koskevia hakuja sormenjälkitietojen perusteella, jotta näiden henkilöllisyys voitaisiin varmistaa paremmin. Euroopan parlamentin ja neuvoston pitäisi hyväksyä säädösehdotus vuoden 2016 kuluessa.

*Horisontaaliset kysymykset*

Tietojärjestelmiin liittyvä yleinen ongelma on niiden **täytäntöönpanoaste** jäsenvaltioissa. Selviä esimerkkejä tästä ovat Prüm-puitteiden epätasainen täytäntöönpano ja tietoliikenneyhteyksien puuttuminen SLTD-tietokantaan. Parantaakseen tietojärjestelmien täytäntöönpanoastetta komissio seuraa tiiviisti kunkin jäsenvaltion suoritustasoa.[23] Seurannassa ei tarkastella vain sitä, ovatko jäsenvaltiot noudattaneet tietojärjestelmiä koskevia oikeudellisia velvoitteitaan, vaan myös sitä, miten ne käyttävät olemassa olevia välineitä ja noudattavatko ne parhaita käytäntöjä. Komissio

[22] COM(2016) 7 final, 19.1.2016.

[23] Ellei Tanskaa koskevassa pöytäkirjassa N:o 22 ja Yhdistynyttä kuningaskuntaa ja Irlantia koskevissa pöytäkirjoissa N:o 21 ja 36 vahvistetuista erityisehdoista muuta johdu.

hankkii täytäntöönpanon seurantaa ja sen edistämistä varten tietoja useista eri lähteistä, kuten jäsenvaltioiden ilmoituksista sekä Schengenin arviointi- ja valvontamekanismin yhteydessä tehtävistä tarkastuskäynneistä.

Toinen tietojärjestelmiin liittyvä yleinen ongelma on niihin **tallennettujen tietojen laatu**. Jos jäsenvaltiot eivät noudata laatua koskevia vähimmäisvaatimuksia, tietojen luotettavuus ja arvo jäävät vähäisiksi, ja virheellisten osumien ja osumien löytymättä jäämisen riski heikentää järjestelmistä saatavaa hyötyä. Tallennettavien tietojen laadun parantamiseksi eu-LISA kehittää kaikkia toimivaltaansa kuuluvia järjestelmiä varten **tietojen laatua koskevan keskitetyn seurantavälineen**.

Useimmissa rajatarkastuksia ja -turvallisuutta koskevissa tietojärjestelmissä käsitellään matkustus- ja henkilöasiakirjoista saatavia tunnistetietoja. Rajaturvallisuuden ja sisäisen turvallisuuden parantaminen edellyttää paitsi toimivia tietojärjestelmiä myös sitä, että matkustus- ja henkilöasiakirjat voidaan todeta oikeiksi helposti ja luotettavasti. Tätä varten komissio esittää toimenpiteitä, joiden tarkoituksena on parantaa **sähköisten asiakirjojen turvallisuutta** ja henkilöllisyyden hallintaa sekä tehostaa asiakirjojen väärentämisen torjuntaa. Yksi keino edistää tätä voisivat olla eIDAS-asetukseen[24] perustuvat luotettavan tunnistamisen yhteentoimivat tasot.

**<u>Toimet nykyisten tietojärjestelmien parantamiseksi</u>**

**Schengenin tietojärjestelmä (SIS)**

- Komissio ja eu-LISA kehittävät ja toteuttavat SIS-järjestelmään sormenjälkien automaattisen tunnistusjärjestelmän (AFIS) vuoden 2017 puoliväliin mennessä.
- Komissio esittää vuoden 2016 loppuun mennessä ehdotukset SIS-järjestelmän oikeusperustan tarkistamisesta sen toimivuuden parantamiseksi.
- Jäsenvaltiot käyttävät SIS-järjestelmää mahdollisimman paljon tallentamalla siihen kaikki tarvittavat tiedot ja tekemällä järjestelmässä hakuja aina tarvittaessa.

**Varastettuja ja kadonneita matkustusasiakirjoja koskeva Interpolin tietokanta (SLTD)**

- Jäsenvaltiot ottavat käyttöön tietoliikenneyhteydet Interpolin välineisiin kaikilla ulkorajojen rajanylityspaikoillaan.
- Jäsenvaltiot noudattavat velvollisuuttaan tallentaa varastettuja ja kadonneita matkustusasiakirjoja koskevat tiedot samanaikaisesti sekä SIS-järjestelmään että SLTD-tietokantaan ja tehdä hakuja niissä molemmissa.

**Matkustajien ennakkotiedot (API)**

- Jäsenvaltiot tarkistavat API-tiedot automaattisesti SIS-järjestelmässä ja SLTD-tietokannassa jo käytössä olevien parhaiden käytäntöjen mukaisesti.
- Komissio arvioi, onko API-tietojen käsittelyä koskevaa oikeusperustaa tarpeen tarkistaa.

**Viisumitietojärjestelmä (VIS)**

- Komissio tutkii vuoden 2016 loppuun mennessä mahdollisuuksia tehdä viisumitietojärjestelmään lisäparannuksia.

[24] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.

**EURODAC**

- Komissio esittää ehdotuksen Eurodacin oikeusperustan tarkistamisesta sen toimintojen tehostamiseksi sääntöjenvastaiseen muuttoliikkeeseen ja palauttamiseen liittyviä tarpeita varten.

**Europol**

- Europol alkaa hyödyntää täysimääräisesti sillä jo olevia oikeuksia tehdä hakuja SIS-, VIS- ja Eurodac-järjestelmässä.
- Komissio ja Europol tutkivat ja edistävät synergiaetuja Europolin tietojärjestelmän (EIS) ja muiden järjestelmien, erityisesti SIS-järjestelmän, välillä.
- Komissio ja eu-LISA selvittävät, voiko SIS-järjestelmää varten kehitettävä sormenjälkien automaattinen tunnistusjärjestelmä (AFIS) täydentää Europolin tietojärjestelmiä rikostutkinta- ja terrorismintorjuntatarkoituksia varten.

**Prüm-puitteet**

- Jäsenvaltiot panevat Prüm-puitteet täytäntöön ja hyödyntävät niitä täysimääräisesti.
- Tarvittaessa komissio käynnistää rikkomusmenettelyt niitä jäsenvaltioita vastaan, jotka eivät ole liittyneet Prüm-puitteisiin.
- Komissio ja eu-LISA selvittävät, voiko SIS-järjestelmää varten kehitettävä sormenjälkien automaattinen tunnistusjärjestelmä (AFIS) täydentää Prüm-puitteiden mukaista sormenjälkitietojen vaihtoa.

**Eurooppalainen rikosrekisteritietojärjestelmä (ECRIS)**

- Euroopan parlamentin ja neuvoston olisi hyväksyttävä vuonna 2016 säädösehdotus, jonka nojalla kansalliset viranomaiset voivat tehdä ECRIS-järjestelmässä kolmansien maiden kansalaisia koskevia hakuja sormenjälkitietojen perusteella.

**Horisontaaliset kysymykset**

- Komissio **seuraa ja pyrkii parantamaan** tietojärjestelmien **täytäntöönpanoastetta**.
- Eu-LISA kehittää kaikkia toimivaltaansa kuuluvia järjestelmiä varten **tietojen laatua koskevan keskitetyn seurantavälineen**.
- Komissio esittää toimenpiteitä, joiden tarkoituksena on parantaa **sähköisten asiakirjojen turvallisuutta ja henkilöllisyyden hallintaa** sekä lujittaa asiakirjojen väärentämisen torjuntaa.
- Komissio tutkii mahdollisuuksia kehittää synergiaetuja ja yhdenmukaisuutta tietojärjestelmien ja niiden toimintainfrastruktuurien välillä EU:n rajaturvallisuuden ja **tullioperaatioiden** alalla.

## 6. UUSIEN TIETOJÄRJESTELMIEN KEHITTÄMINEN JA PUUTTEIDEN KORJAAMINEN

Vaikka nykyiset tietojärjestelmät kattavat hyvin laajalti erilaisia tietoja, joita tarvitaan rajaturvallisuuteen ja lainvalvontaan liittyvässä työssä, niissä on myös merkittäviä puutteita. Komissio on jo pyrkinyt korjaamaan osan näistä puutteista esittämällä säädösehdotuksia, jotka koskevat muun muassa rajanylitystietojärjestelmää ja EU:n matkustajarekisteritietojärjestelmää. Muiden havaittujen puutteiden osalta olisi harkittava tarkkaan, tarvitaanko niiden korjaamiseksi uusia EU:n välineitä.

### 1. Rajanylitystietojärjestelmä

Komissio on esittänyt tarkistetut säädösehdotukset rajanylitystietojärjestelmän (Entry-Exit System, EES) perustamiseksi samaan aikaan tämän tiedonannon kanssa. Sen jälkeen

kun lainsäätäjät ovat hyväksyneet ehdotuksen, eu-LISAn tehtävänä on kehittää ja toteuttaa järjestelmä yhteistyössä Schengeniin osallistuvien jäsenvaltioiden kanssa.

Rajanylitystietojärjestelmään kirjataan kaikkien kolmansien maiden kansalaisten rajanylitykset, kun nämä vierailevat Schengen-alueella lyhytaikaisesti (enintään 90 päivän ajan minkä tahansa 180 päivän jakson aikana), olipa kyse viisumivelvollisista tai viisumivaatimuksesta vapautetuista matkustajista, tai kun nämä oleskelevat alueella kiertomatkaviisumin nojalla (enintään yhden vuoden ajan). Rajanylitystietojärjestelmän tarkoituksena on a) parantaa ulkorajojen turvallisuutta, b) vähentää sääntöjenvastaista muuttoliikettä puuttumalla sallitun oleskeluajan ylittämiseen ja c) edistää terrorismin ja vakavan rikollisuuden torjuntaa ja tukea siten sisäisen turvallisuuden korkean tason varmistamista.

Rajanylitystietojärjestelmään tallennetaan kolmansien maiden kansalaisten henkilöllisyyttä koskevat tiedot (alfanumeeriset tiedot, neljä sormenjälkeä ja kasvokuva) sekä heidän matkustusasiakirjojensa tiedot ja yhdistetään nämä sähköisiin rajanylitystietoihin. Nykyään käytössä oleva matkustusasiakirjojen leimaaminen lopetetaan. Rajanylitystietojärjestelmän ansiosta sallittua lyhytaikaista oleskelua voidaan hallinnoida tehokkaammin ja automaatiota rajatarkastuksissa lisätä. Lisäksi väärennettyjen asiakirjojen ja henkilöllisyyspetosten paljastaminen helpottuu. Keskitetyn tallentamisen ansiosta voidaan paljastaa sekä sallitun oleskeluajan ylittäneet henkilöt että ne, jotka oleskelevat Schengen-alueella ilman asianmukaisia asiakirjoja. Näin ehdotettu rajanylitystietojärjestelmä auttaa korjaamaan nykyisissä tietojärjestelmissä olevan merkittävän puutteen.

## 2. Matkustajarekisteritiedot

Matkustajarekisteritiedot (Passenger Name Record, PNR) muodostuvat varaustiedoista, joihin kuuluvat matkustajan yhteystiedot, kaikki matkaa ja varausta koskevat tiedot, erityishuomautukset, paikka- ja matkatavaratiedot sekä maksuvälinetiedot. Matkustajarekisteritietoja tarvitaan, koska niiden avulla voidaan tunnistaa korkean riskin matkustajia terrorismin, huumekaupan, ihmiskaupan, lasten seksuaalisen hyväksikäytön ja muiden vakavien rikosten torjuntaa varten. Ehdotetun matkustajarekisteridirektiivin avulla voidaan varmistaa parempi yhteistyö kansallisten järjestelmien kesken ja vähentää turvallisuusvajeita jäsenvaltioiden välillä. Ehdotettu matkustajarekisteridirektiivi täyttää näin ollen merkittävän aukon tietojen saatavuudessa. Tämä on tarpeen vakavan rikollisuuden ja terrorismin torjunnassa. **Matkustajarekisteridirektiivi olisi hyväksyttävä ja pantava täytäntöön pikimmiten**.

Ehdotetussa direktiivissä säädetään, että jäsenvaltioiden on perustettava matkustajatietoyksiköitä, jotka keräävät PNR-tiedot lentoliikenteen harjoittajilta. Tätä varten ei ole tarkoitus perustaa keskitettyä järjestelmää tai tietokantaa, vaan kansallisia teknisiä ratkaisuja ja menettelyjä vain yhdenmukaistetaan tietyiltä osin. Tämä helpottaa PNR-tietojen vaihtoa matkustajatietoyksiköiden kesken ehdotetussa direktiivissä säädetyllä tavalla. Komissio tukee jäsenvaltioita analysoimalla tätä varten erilaisia skenaarioita, joiden mukaisesti matkustajatietoyksiköt voisivat olla yhteydessä toisiinsa. Tarkoituksena on tarjota yhdenmukaisia ratkaisuja ja menettelyjä. Direktiivin hyväksymisen jälkeen komissio kiirehtii toimia, joiden avulla toteutetaan yhteiset yhteyskäytännöt ja tuetut tietomuodot PNR-tietojen siirtämiseksi lentoliikenteen harjoittajilta matkustajatietoyksiköihin. Komissio laatii luonnoksen täytäntöönpanosäädökseksi kolmen kuukauden kuluessa direktiivin hyväksymisestä.

## 3. Ennakkotietojen puuttuminen viisumivaatimuksesta vapautetuista kolmansien maiden kansalaisista

Viisuminhaltijoiden henkilöllisyys, yhteystiedot ja tausta kirjataan viisumitietojärjestelmään, mutta ainoat tiedot viisumivaatimuksesta vapautetuista henkilöistä ovat peräisin heidän matkustusasiakirjoistaan. Lento- tai meriteitse saapuvien matkustajien osalta voidaan lisäksi saada API-tietoja ennen heidän saapumistaan EU:n alueelle. Ehdotetun matkustajarekisteridirektiivin mukaan heiltä kerättäisiin myös PNR-tiedot, jos he saapuvat EU:hun lentäen. Sen sijaan EU:n alueelle maarajojen kautta tulevista henkilöistä ei ole saatavilla mitään tietoja ennen heidän saapumistaan EU:n ulkorajalle.

Lainvalvontaviranomaiset voivat saada viisuminhaltijoista tietoja viisumitietojärjestelmästä, jos se on tarpeen vakavan rikollisuuden ja terrorismin torjuntaa varten, mutta viisumivaatimuksesta vapautetuista henkilöistä ei ole saatavilla vastaavia tietoja. Tämä tiedonpuute koskee erityisesti EU:n maarajojen valvontaa tilanteessa, jossa näille rajoille saapuu huomattavia määriä viisumivaatimuksesta vapautettuja matkustajia henkilöautoilla, linja-autoilla ja junalla. Useiden EU:n naapurimaiden kansalaiset on jo vapautettu viisumivaatimuksesta, ja EU:n ja muiden naapurimaiden välillä käydään viisumivapautta koskevia vuoropuheluja. Tämä todennäköisesti lisää viisumivaatimuksesta vapautettujen matkustajien määrää huomattavasti jo lähitulevaisuudessa.

Komissio arvioi, olisiko uuden EU:n välineen kehittäminen tätä varten tarpeellista, mahdollista tai oikeasuhteista. Yhtenä vaihtoehtona voitaisiin harkita **EU:n matkustustieto- ja lupajärjestelmää (ETIAS)**, johon viisumivapautetut matkustajat rekisteröisivät tarvittavat tiedot suunnitellusta matkastaan. Näiden tietojen automaattisesta käsittelystä olisi apua rajavartijoille lyhytaikaista oleskelua varten saapuvien kolmansien maiden kansalaisten arvioimisessa. Esimerkiksi Yhdysvallat, Kanada ja Australia ovat jo ottaneet käyttöön tämäntyyppisiä järjestelmiä, jotka koskevat myös EU:n kansalaisia.

Matkustuslupajärjestelmät perustuvat verkossa tehtäviin hakemuksiin, joissa hakija ilmoittaa ennen lähtöä muun muassa henkilö- ja yhteystietonsa sekä matkan tarkoituksen ja reitin. Kun matkustuslupa on myönnetty, rajamenettelyt maahan saapuessa sujuvat nopeammin ja helpommin. Sen lisäksi, että tällaisesta järjestelmästä olisi hyötyä turvallisuuden ja rajavalvonnan ja kenties myös vastavuoroisten viisumivapautusten kannalta, se myös helpottaisi matkustamista.

## 4. Eurooppalainen poliisirekisteritietojärjestelmä (EPRIS)

Kuten Euroopan turvallisuusagendassa todetaan, tietojenvaihdon kehittämisen yhteydessä olisi parannettava poliisitietojen reaaliaikaista saatavuutta jäsenvaltioiden välillä. Komissio arvioi, olisiko tarpeellista, teknisesti toteuttamiskelpoista ja oikeasuhteista kehittää eurooppalainen poliisirekisteritietojärjestelmä (EPRIS), jonka avulla voitaisiin helpottaa rajat ylittävää pääsyä kansallisiin lainvalvontatietokantoihin. Komissio myöntää tätä varten EU-rahoitusta viiden jäsenvaltion ryhmän toteuttamaan kokeiluhankkeeseen, jonka tarkoituksena on kehittää mekanismi kansallisissa indekseissä tehtäviä automaattisia rajatylittäviä hakuja varten osuma / ei osumaa -periaatteella.[25] Komissio ottaa arvioinnissaan huomioon tämän hankkeen tulokset.

[25] Automaattista tietojenvaihtoprosessia (ADEP) koskevan pilottihankkeen tarkoituksena on luoda tekninen järjestelmä, jonka avulla voidaan indeksiä käyttäen selvittää, onko tietystä henkilöstä tai rikospoliisin tutkinnasta saatavilla poliisitietoja yhdessä tai useammassa muussa jäsenvaltiossa.

**Toimet uusien tietojärjestelmien kehittämiseksi ja tiedoissa olevien aukkojen poistamiseksi**

**Rajanylitystietojärjestelmä (EES)**

- Euroopan parlamentin ja neuvoston olisi käsiteltävä rajanylitystietojärjestelmää koskevat säädösehdotukset erittäin kiireellisinä, jotta ne voitaisiin hyväksyä ennen vuoden 2016 loppua.

**Matkustajarekisteritiedot (PNR)**

- Euroopan parlamentin ja neuvoston olisi hyväksyttävä matkustajarekisteridirektiivi viimeistään huhtikuussa 2016.
- Jäsenvaltioiden olisi pantava matkustajarekisteridirektiivi täytäntöön kiireellisesti heti sen hyväksymisen jälkeen.
- Komissio tukee tietojenvaihtoa matkustajatietoyksikköjen välillä yhdenmukaisten ratkaisujen ja menettelyjen avulla.
- Komissio laatii luonnoksen täytäntöönpanopäätökseksi, joka koskee yhteisiä yhteyskäytäntöjä ja tuettuja tietomuotoja PNR-tietojen siirtämiseksi lentoliikenteen harjoittajilta matkustajatietoyksiköihin, kolmen kuukauden kuluessa siitä kun matkustajarekisteridirektiivi on hyväksytty.

**Ennakkotietojen puuttuminen viisumivaatimuksesta vapautetuista kolmansien maiden kansalaisista**

- Komissio arvioi vuonna 2016, olisiko uuden EU:n välineen, kuten EU:n matkustustieto- ja lupajärjestelmän, kehittäminen tarpeellista, teknisesti mahdollista ja oikeasuhteista.

**Eurooppalainen poliisirekisteritietojärjestelmä (EPRIS)**

- Komissio arvioi vuonna 2016, olisiko eurooppalaisen poliisirekisteritietojärjestelmän perustaminen tarpeellista, teknisesti mahdollista ja oikeasuhteista.

## 7. TAVOITTEENA TIETOJÄRJESTELMIEN YHTEENTOIMIVUUS

Yhteentoimivuudella tarkoitetaan mahdollisuutta vaihtaa ja jakaa tietoja tietojärjestelmien välillä. Yhteentoimivuus voidaan toteuttaa **neljällä eri tavalla**, joista jokaiseen liittyy erilaisia oikeudellisia[26], teknisiä ja operatiivisia ongelmia muun muassa tietosuojan kannalta:

- yhteinen hakuliittymä, jonka kautta voidaan tehdä hakuja useissa tietojärjestelmissä samanaikaisesti ja esittää yhdistetyt hakutulokset samassa näkymässä
- tietojärjestelmien yhteenliitettävyys, jonka ansiosta järjestelmä tekee automaattisesti haun toiseen järjestelmään tallennettujen tietojen perusteella
- yhteisen biometrisen tunnistuspalvelun perustaminen useiden eri tietojärjestelmien tueksi
- eri tietojärjestelmien yhteinen tietovarasto (keskusmoduuli).

---

Indeksissä tehtävään automaattiseen hakuun saatu vastaus osoittaisi osuma / ei osumaa -periaatteen mukaisesti vain sen, onko tietoja saatavilla vai ei. Osuman saamisen jälkeen muut henkilötiedot olisi pyydettävä erikseen seuraavassa vaiheessa tavanomaisia poliisiyhteistyön kanavia käyttäen.

[26] Ellei Tanskaa koskevassa pöytäkirjassa N:o 22 ja Yhdistynyttä kuningaskuntaa ja Irlantia koskevissa pöytäkirjoissa N:o 21 ja 36 vahvistetuista erityisehdoista muuta johdu.

Komissio perustaa tietojärjestelmien yhteentoimivuuteen tähtäävän työn käynnistämiseksi **tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän korkean tason asiantuntijaryhmän** yhdessä EU:n virastojen, kansallisten asiantuntijoiden ja institutionaalisten sidosryhmien kanssa. Ryhmän tehtävänä on käsitellä tietojärjestelmien yhteentoimivuuden toteuttamista koskeviin eri vaihtoehtoihin liittyviä oikeudellisia, teknisiä ja operatiivisia näkökohtia sekä eri vaihtoehtojen tarpeellisuutta, teknistä toteutettavuutta ja oikeasuhteisuutta sekä niiden vaikutuksia tietosuojaan. Ryhmän olisi käsiteltävä havaittuja puutteita ja tiedoissa olevia aukkoja, jotka johtuvat EU:n tason tietojärjestelmien monimutkaisuudesta ja hajanaisuudesta. Ryhmän on tarkasteltava rajaturvallisuutta ja lainvalvontaa laajasti ja kattavasti, ottaen huomioon myös niihin liittyvät tulliviranomaisten tehtävät, vastuualueet ja järjestelmät. Ryhmän työssä pyritään yhdistämään kaikki tähän liittyvät kokemukset, joita tähän asti on liian usein kehitetty siiloajattelun pohjalta.

Prosessin tavoitteena on luoda strateginen kokonaisnäkemys EU:n tietoarkkitehtuurista rajaturvallisuuden ja sisäisen turvallisuuden alalla sekä tarjota ratkaisuja sen toteuttamista varten.

Tätä kuulemisprosessia **ohjaavat seuraavat tavoitteet**:

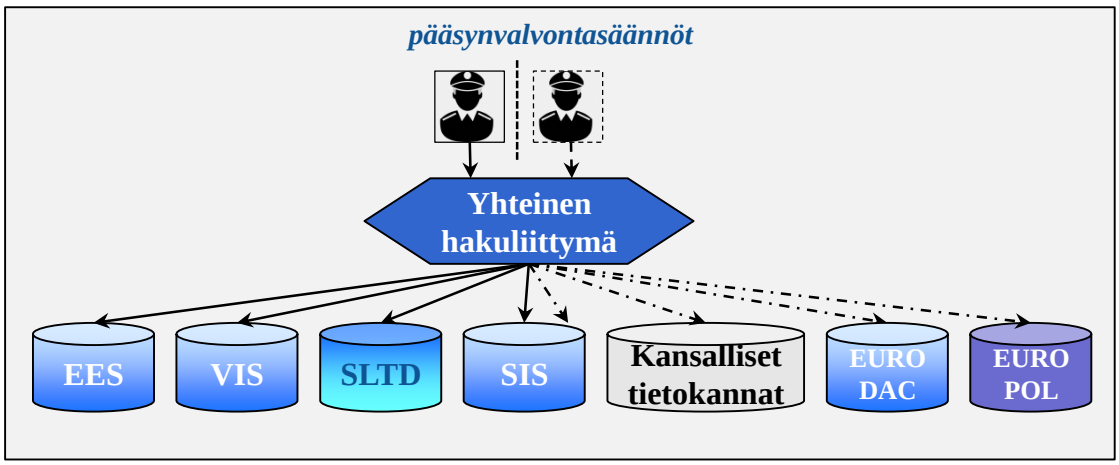
- Tietojärjestelmien olisi täydennettävä toisiaan. Päällekkäisyyksiä olisi vältettävä, ja olemassa olevat päällekkäisyydet olisi poistettava. Tiedoissa olevat aukot olisi täytettävä asianmukaisella tavalla.
- Olisi noudatettava modulaarista lähestymistapaa, jossa hyödynnetään täysimääräisesti tekniikan kehitystä ja noudatetaan sisäänrakennetun yksityisyyden suojan periaatetta.
- Sekä unionin että kolmansien maiden kansalaisten perusoikeuksien täysimääräinen kunnioittaminen olisi varmistettava alusta alkaen perusoikeuskirjan mukaisesti.
- Tietojärjestelmät olisi tarvittaessa ja mahdollisuuksien mukaan yhdistettävä toisiinsa ja niiden olisi oltava yhteentoimivia. Olisi helpotettava hakujen tekemistä useissa järjestelmissä samanaikaisesti sen varmistamiseksi, että rajavartijat ja/tai poliisit saavat kaikki tarvittavat tiedot juuri silloin kun ja juuri siellä missä he niitä tarvitsevat tehtäviensä hoitamista varten, jo myönnettyjä pääsyoikeuksia muuttamatta.

## 1. Yhteinen hakuliittymä

Yksi keino toteuttaa tietojärjestelmien yhteentoimivuus on tarjota sekä rajavartijoille että poliiseille, näiden pääsyoikeuksia täysimääräisesti kunnioittaen ja näiden tehtäviin liittyviä tarkoituksia varten, **mahdollisuus tehdä hakuja useassa tietojärjestelmässä samanaikaisesti niin, että yhdistetyt tulokset esitetään samassa näkymässä**. Tätä varten tarvitaan alustoja, joissa on yksi yhteinen hakuliittymä ja joiden avulla tietojärjestelmissä voidaan tehdä hakuja samanaikaisesti yhdellä komennolla. Tällainen alusta voisi tehdä hakuja useassa tietokannassa samanaikaisesti esimerkiksi matkustusasiakirjan mikrosirun tai biometristen tietojen perusteella. Yhteinen hakutoiminto olisi kaikkien niiden viranomaisten käytettävissä, jotka tarvitsevan pääsyn kyseisiin tietoihin ja oikeuden käyttää niitä (esimerkiksi rajavartijat, lainvalvontaviranomaiset, turvapaikkapalvelut) käyttötarkoituksen rajoittamisen ja tiukkojen pääsynvalvontasääntöjen mukaisesti. Hakuja voisi tehdä myös mobiililaitteilla. Yhteinen hakuliittymä vähentäisi tietojärjestelmien monimutkaisuutta EU:n tasolla, koska sen ansiosta rajavartijat ja poliisit voisivat tehdä hakuja samanaikaisesti monessa tietojärjestelmässä omien käyttöoikeuksiensa puitteissa.

Useissa jäsenvaltioissa on jo otettu käyttöön tällaisia alustoja, joissa on yhteinen hakuliittymä. Komissio ja eu-LISA pyrkivät tämän vallitsevan hyvän käytännön pohjalta laatimaan yhdenmukaisen ratkaisun yhteistä hakuliittymää varten. Jäsenvaltioiden olisi hyödynnettävä tällaisten toimintojen asentamista varten sisäisen turvallisuuden rahaston kansallisesta ohjelmasta saatavaa EU:n rahoitusta. Komissio seuraa tiiviisti yhteisen hakuliittymän käyttöä jäsenvaltioissa kansallisella tasolla.

***Kaavio 2** Yhteinen hakuliittymä*




On helpompaa tehdä hakuja useissa keskitetyissä tai kansallisissa järjestelmissä (ks. kaavio) kuin hajautetuissa järjestelmissä. Komissio ja eu-LISA selvittävät, voitaisiinko yhteisen hakuliittymän avulla tehdä samanaikaisesti keskitettyjä hakuja myös hajautetuissa järjestelmissä, kuten Prüm- ja ECRIS-järjestelmissä. Komissio ja eu-LISA laativat tämän analyysin yhdessä tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän asiantuntijaryhmän kanssa, jo myönnettyjä pääsyoikeuksia muuttamatta.

**2. Tietojärjestelmien yhteenliitettävyys**

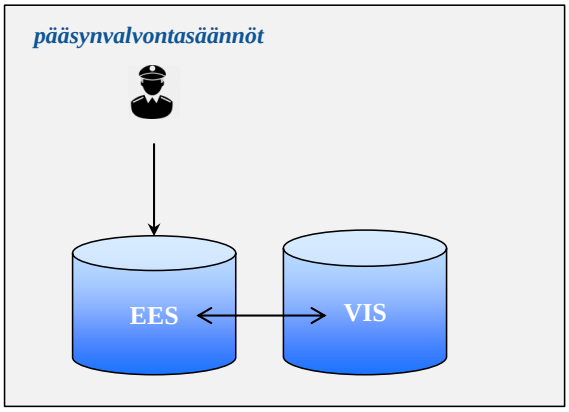
Toinen keino varmistaa tietojärjestelmien yhteentoimivuus on niiden yhteenliitettävyys. Se tarkoittaa, että erilaiset järjestelmät tai tietokannat pystyvät kommunikoimaan keskenään teknisesti. **Järjestelmä pystyisi tekemään keskustasolla automaattisesti haun johonkin toiseen järjestelmään tallennettujen tietojen perusteella.** Tämä edellyttää, että järjestelmät ovat teknisesti yhteensopivia ja että niihin tallennettavat tietoalkiot (esimerkiksi sormenjäljet) ovat yhteentoimivia. Yhteenliitettävyyden ansiosta on mahdollista vähentää viestintäverkoissa liikkuvan ja kansallisten järjestelmien kautta siirrettävän datan määrää.

Yhteenliitettävyys edellyttää asianmukaisia tietosuojatakeita ja tiukkoja pääsynvalvontasääntöjä. Lainsäätäjät saavuttivat joulukuussa 2015 poliittisen yhteisymmärryksen tietosuojauudistuksesta, joten kaikkialla EU:ssa saadaan käyttöön uudenaikainen tietosuojakehys, joka sisältää tällaiset takeet. On tärkeää, että lainsäätäjät hyväksyvät yleisen tietosuoja-asetuksen ja tietosuojadirektiivin viipymättä.

Yhteenliitettävyys on otettu huomioon tulevassa rajanylitystietojärjestelmässä. Se pystyy kommunikoimaan suoraan viisumitietojärjestelmän kanssa keskustasolla ja päinvastoin. Tämä on merkittävä edistysaskel rajaturvallisuuden ja sisäisen turvallisuuden alalla käytössä olevan EU:n tietoarkkitehtuurin hajanaisuuden ja siitä aiheutuvien ongelmien korjaamisessa. Automaattisen ristiintarkistuksen ansiosta jäsenvaltioiden ei tarvitse tehdä

rajatarkastusten yhteydessä erikseen hakuja viisumitietojärjestelmään, minkä lisäksi ylläpitotarve vähenee ja järjestelmän suorituskyky paranee.

***Kaavio 3*** *Tietojärjestelmien yhteenliitettävyys: esimerkkinä EES/VIS*



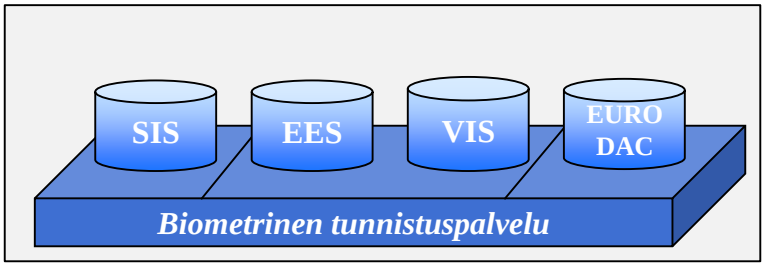

Seuraavaksi komissio ja eu-LISA analysoivat, voitaisiinko tulevan EES-järjestelmän ja VIS-järjestelmän keskustason yhteenliitettävyyttä laajentaa SIS-järjestelmään ja voisiko se toimia myös Eurodac- ja SIS-järjestelmien välillä. Komissio ja eu-LISA laativat tämän analyysin yhdessä tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän asiantuntijaryhmän kanssa.

### 3. Yhteinen biometrinen tunnistuspalvelu

Kolmas keino toteuttaa tietojärjestelmien yhteentoimivuus perustuu biometristen tunnisteiden käyttöön. Kun sormenjäljet otetaan esimerkiksi jonkin jäsenvaltion konsulaatissa tietynlaisella laitteella, on olennaisen tärkeää, että niitä voidaan vertailla viisumitietojärjestelmässä käyttäen toisenlaista laitetta jonkin toisen jäsenvaltion raja-asemalla. Tämä vaatimus koskee myös muissa järjestelmissä tehtäviä sormenjälkihakuja: biometristen näytteiden on täytettävä tietyt laatua ja muotoa koskevat vähimmäisvaatimukset, jotta tämäntyyppinen yhteentoimivuus voi toteutua ongelmitta.

Järjestelmätasolla biometristen tunnisteiden yhteentoimivuus mahdollistaa useiden tietojärjestelmien yhteisen biometrisen tunnistuspalvelun käytön. Samalla noudatetaan henkilötietojen suojaa koskevia sääntöjä jakamalla tiedot eri osastoihin niin, että kuhunkin tietoluokkaan sovelletaan erillisiä pääsynvalvontasääntöjä.[27] Tällaisista yhteisistä palveluista saadaan merkittäviä taloudellisia sekä ylläpitoon ja toimintaan liittyviä etuja.

***Kaavio 4*** *Yhteinen biometrinen tunnistuspalvelu*




[27] Samaan tapaan kuin useat eri käyttäjät voivat käyttää saman fyysisen tiedostopalvelimen eri kansioita kukin omien käyttöoikeuksiensa mukaisesti.

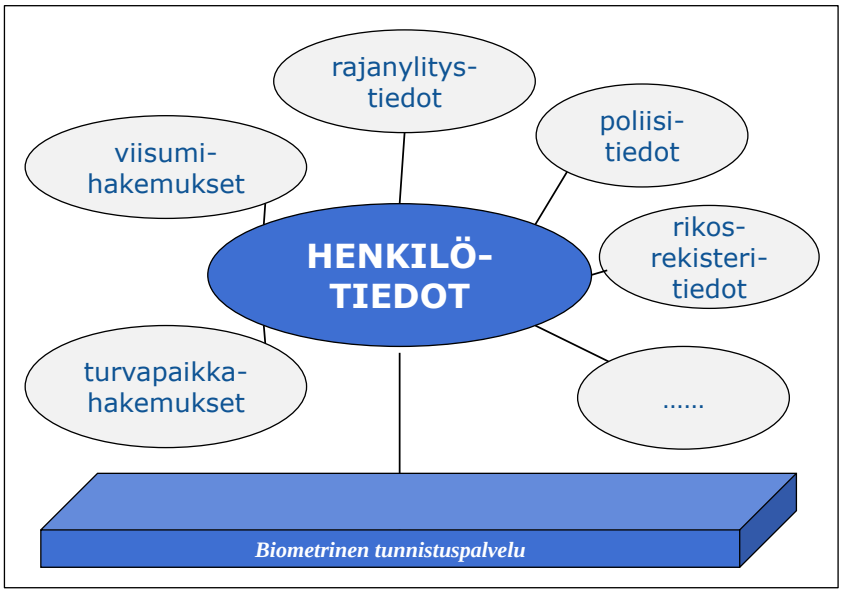
Komissio ja eu-LISA selvittävät, olisiko yhteinen biometrinen tunnistuspalvelu otettava käyttöön kaikkien asianomaisten tietojärjestelmien yhteydessä ja olisiko tämä teknisesti toteutettavissa. Komissio ja eu-LISA laativat analyysin yhdessä tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän asiantuntijaryhmän kanssa.

## 4. Yhteinen tietovarasto

Kunnianhimoisin pitkän aikavälin lähestymistapa yhteentoimivuuden toteuttamiseen olisi **EU:n eri tietojärjestelmien yhteisen tietovaraston** perustaminen. Yhteinen tietovarasto muodostaisi keskusmoduulin, joka sisältäisi perustiedot (alfanumeeriset ja biometriset tiedot), kun taas muut tietoalkiot ja eri tietojärjestelmien erityispiirteet (esim. viisumitiedot) tallennettaisiin omiin moduuleihinsa. Keskusmoduuli ja erityismoduulit yhdistettäisiin keskenään niin, että eri tietokokonaisuudet linkittyisivät toisiinsa. Näin syntyisi **modulaarinen yhdennetty henkilöllisyyden hallinta rajaturvallisuuden ja sisäisen turvallisuuden tueksi**. Tietosuojasääntöjen noudattaminen olisi varmistettava esimerkiksi jakamalla tiedot eri osastoihin niin, että kuhunkin tietoluokkaan sovellettaisiin erillisiä pääsynvalvontasääntöjä.

Yhteinen tietovarasto voisi tuoda ratkaisun rajaturvallisuuden ja sisäisen turvallisuuden alalla käytössä olevan EU:n tietoarkkitehtuurin hajanaisuuteen. Tämä hajanaisuus on ristiriidassa sen periaatteen kanssa, että tietoja pitäisi kerätä mahdollisimman vähän, koska sen seurauksena samoja tietoja tallennetaan moneen kertaan. Yhteisen tietovaraston avulla voitaisiin tarvittaessa havaita yhteyksiä ja luoda kokonaiskuva yhdistämällä eri tietojärjestelmiin tallennettuja yksittäisiä tietoalkioita. Näin sen avulla voitaisiin korjata tiedoissa olevia aukkoja ja antaa rajavartijoille ja poliisille paremmat mahdollisuudet tehdä havaintoja katvealueilla.

***Kaavio 5*** *Yhteinen tietovarasto*




Yhteisen tietovaraston perustaminen EU:n tasolla herättää merkittäviä kysymyksiä siihen liittyvän tietojenkäsittelyn tarkoituksen määrittelystä, tarpeellisuudesta, teknisestä toteutettavuudesta ja oikeasuhteisuudesta. Se edellyttäisi eri tietojärjestelmien perustamista koskevan oikeudellisen kehyksen kokonaistarkistusta, mikä voitaisiin toteuttaa vain pitkällä aikavälillä. Tietojärjestelmiä ja niiden yhteentoimivuutta

käsittelevä asiantuntijaryhmä tarkastelee yhteiseen tietovarastoon liittyviä oikeudellisia, teknisiä ja operatiivisia kysymyksiä, tietosuojaan liittyvät kysymykset mukaan lukien.

Kaikki edellä mainitut yhteentoimivuuden toteuttamistavat (yhteinen hakuliittymä, järjestelmien yhteenliitettävyys, yhteinen biometrinen tunnistuspalvelu ja yhteinen tietovarasto) edellyttävät, että eri tietojärjestelmiin tai moduuleihin tallennettavat tiedot ovat keskenään yhteentoimivia. Tätä silmällä pitäen on tärkeää jatkaa ns. **standardiviestimuotoon** (Uniform Message Format, UMF) liittyvää työtä, jotta kaikille tietojärjestelmille voidaan luoda yhteiset säännöt.[28]

**Toimet tietojärjestelmien yhteentoimivuuden toteuttamiseksi**

- Komissio perustaa yhdessä EU:n virastojen, jäsenvaltioiden ja asianomaisten sidosryhmien kanssa **tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän asiantuntijaryhmän**, jonka tehtävänä on tutkia tietojärjestelmien yhteentoimivuuteen liittyviä oikeudellisia, teknisiä ja operatiivisia näkökohtia, kuten eri vaihtoehtojen tarpeellisuutta, teknistä toteutettavuutta ja oikeasuhteisuutta sekä niistä aiheutuvia vaikutuksia tietosuojan kannalta.

**Yhteinen hakuliittymä**

- Komissio ja eu-LISA tukevat jäsenvaltioita yhteisen hakuliittymän asentamisessa keskustietojärjestelmiin tehtäviä hakuja varten.
- Komissio ja eu-LISA selvittävät yhdessä asiantuntijaryhmän kanssa, voitaisiinko yhteistä hakuliittymää käyttää keskitettyjen hakujen tekemiseen kaikissa asianomaisissa järjestelmissä samanaikaisesti, jo myönnettyjä pääsyoikeuksia muuttamatta.

**Tietojärjestelmien yhteenliitettävyys**

- Komissio ja eu-LISA selvittävät yhdessä asiantuntijaryhmän kanssa, voitaisiinko keskitettyjen tietojärjestelmien yhteenliitettävyys toteuttaa kattavammin kuin tähän mennessä on ehdotettu rajanylitystietojärjestelmän ja viisumitietojärjestelmän yhteydessä.

**Biometrinen tunnistuspalvelu**

- Komissio ja eu-LISA selvittävät yhdessä asiantuntijaryhmän kanssa, olisiko tarpeellista ja teknisesti mahdollista toteuttaa kaikki asianomaiset tietojärjestelmät kattava yhteinen biometrinen tunnistuspalvelu.

**Yhteinen tietovarasto (keskusmoduuli)**

- Komissio ja eu-LISA selvittävät yhdessä asiantuntijaryhmän kanssa yhteisen tietovaraston pitkän aikavälin kehittämiseen liittyviä oikeudellisia, teknisiä, operatiivisia ja taloudellisia vaikutuksia.
- Komissio ja eu-LISA jatkavat vireillä olevaa työtä yhteisen standardiviestimuodon kehittämiseksi kaikkia asianomaisia tietojärjestelmiä varten.

[28] Komissio on kannattanut standardiviestimuodon jatkokehittämistä vuonna 2012 antamassaan eurooppalaista tiedonvaihtomallia (EIXM) koskevassa tiedonannossa. Se rahoittaa parhaillaan kolmatta tähän liittyvää pilottihanketta, jonka tavoitteena on luoda kaikille tietokannoille yhteinen standardi, jota käytettäisiin sekä kansallisella tasolla (jäsenvaltioissa) ja EU:n tasolla (keskitetyissä järjestelmissä ja virastoissa) että kansainvälisellä tasolla (Interpolissa).

## 8. PÄÄTELMÄT

Tämän tiedonannon tarkoituksena on käynnistää keskustelu siitä, miten EU:n tietojärjestelmien avulla voitaisiin parantaa rajaturvallisuutta ja sisäistä turvallisuutta Euroopan turvallisuus- ja muuttoliikeagendojen merkittäviä synergiaetuja hyödyntäen. Rajavartijat ja poliisit voivat jo nyt saada tarvitsemiaan tietoja useista eri tietojärjestelmistä, mutta nämä järjestelmät eivät ole täydellisiä. EU:n haasteena on kehittää vahvempi ja älykkäämpi tietoarkkitehtuuri, noudattaen täysimääräisesti perusoikeuksia ja erityisesti henkilötietojen suojaa ja tietojen käyttötarkoituksen rajoittamisen periaatetta.

EU:n tietoarkkitehtuurissa olevat aukot on korjattava. Komissio esittää samaan aikaan tämän tiedonannon kanssa rajanylitystietojärjestelmän perustamista koskevan ehdotuksen, joka olisi hyväksyttävä kiireellisesti. Myös matkustajarekisteridirektiivi olisi hyväksyttävä lähiviikkojen aikana. Ennen kesää olisi hyväksyttävä myös Euroopan raja- ja rannikkovartiostoa koskeva ehdotus. Samalla komissio jatkaa työtä, jonka puitteissa vahvistetaan ja tarvittaessa virtaviivaistetaan olemassa olevia järjestelmiä, muun muassa kehittämällä Schengenin tietojärjestelmään liitettävä sormenjälkien automaattinen tunnistusjärjestelmä.

Jäsenvaltioiden on käytettävä nykyisiä tietojärjestelmiä täysimääräisesti ja otettava käyttöön tarvittavat tekniset yhteydet kaikkiin tietojärjestelmiin ja tietokantoihin oikeudellisten velvoitteidensa mukaisesti. Muun muassa Prüm-puitteissa havaitut puutteet on korjattava viipymättä. Samalla kun tällä tiedonannolla käynnistetään keskustelu ja prosessi järjestelmissä havaittujen puutteiden ja ongelmien korjaamiseksi, jäsenvaltioiden on kiireellisesti korjattava EU:n tietokantojen täydentämisessä ja tietojenvaihdossa unionin alueella havaitut puutteet.

Tällä tiedonannolla käynnistetään prosessi tietojärjestelmien yhteentoimivuuden toteuttamiseksi, jotta rajaturvallisuuteen ja sisäiseen turvallisuuteen liittyvän EU:n tietoarkkitehtuurin rakennetta voitaisiin parantaa. Komissio perustaa tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän asiantuntijaryhmän, jonka tehtävänä on tutkia tietojärjestelmien yhteentoimivuuden toteuttamista koskeviin vaihtoehtoihin liittyviä oikeudellisia, teknisiä ja operatiivisia näkökohtia ja puuttua havaittuihin puutteisiin ja ongelmiin. Asiantuntijaryhmän työn perusteella komissio esittää Euroopan parlamentille ja neuvostolle konkreettisia ehdotuksia pohjaksi yhteiselle keskustelulle siitä, miten asiassa olisi edettävä. Komissio pyytää tähän pohdintaan panosta myös Euroopan tietosuojavaltuutetulta ja tietosuojatyöryhmässä kokoontuvilta kansallisilta tietosuojaviranomaisilta.

Tavoitteena on kehittää yhteinen strategia, jonka avulla EU:n tiedonhallinnasta voidaan tehdä tehokkaampaa ja tuloksellisempaa tietosuojaan liittyviä vaatimuksia täysimääräisesti noudattaen, jotta unionin ulkorajoja voidaan suojella paremmin ja parantaa sisäistä turvallisuutta kaikkien kansalaisten edun mukaisesti.

## LIITE 1: LYHENTEET

| | |
|---|---|
| API | matkustajien ennakkotiedot |
| AFIS | sormenjälkien automaattinen tunnistusjärjestelmä, jota käytetään sormenjälkien ottamisessa, tallentamisessa, vertailussa ja tarkistamisessa. |
| CIS | tullitietojärjestelmä |
| ECRIS | eurooppalainen rikosrekisteritietojärjestelmä |
| EES | rajanylitystietojärjestelmä (ehdotus) |
| EIXM | eurooppalainen tiedonvaihtomalli |
| EIS | Europolin tietojärjestelmä |
| EPRIS | eurooppalainen poliisirekisteritietojärjestelmä |
| EURODAC | järjestelmä sormenjälkitietojen vertailua varten |
| Europol | Euroopan poliisivirasto (Euroopan unionin lainvalvontavirasto) |
| ETIAS | EU:n matkustustieto- ja lupajärjestelmä (mahdollinen) |
| eu-LISA | vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto |
| FIND | Interpolin tietokanta |
| Frontex | Euroopan unionin jäsenvaltioiden operatiivisesta ulkorajayhteistyöstä huolehtiva virasto |
| iARMS | Interpolin sähköinen laittomien aseiden rekisteröinnin ja jäljityksen hallintajärjestelmä |
| Interpol | Kansainvälinen rikospoliisijärjestö |
| MIND | Interpolin tietokanta |
| PIU | matkustajatietoyksikkö: perustetaan kuhunkin jäsenvaltioon keräämään PNR-tiedot lentoliikenteen harjoittajilta |
| PNR | matkustajarekisteritiedot |
| Prüm | poliisiyhteistyön väline, jonka avulla vaihdetaan DNA- ja sormenjälkitietoja sekä ajoneuvojen rekisteröintitietoja |
| SafeSeaNet | EU:n merenkulun sähköinen tiedonvaihtojärjestelmä jäsenvaltioiden merenkulkuviranomaisten käyttöön |
| SBC | Schengenin rajasäännöstö |
| SIENA | suojattu tiedonvaihtoverkkosovellus |
| SIS | Schengenin tietojärjestelmä (joskus myös toisen sukupolven Schengenin tietojärjestelmä, SIS II) |
| SLTD | varastettuja ja kadonneita matkustusasiakirjoja koskeva Interpolin tietokanta |
| sTESTA | Euroopan laajuinen julkishallinnon suojattu tietoliikenneverkko (seuraava sukupolvi TESTA-NG) |
| UMF | standardiviestimuoto, jonka avulla varmistetaan tietojärjestelmien yhteensopivuus |
| VIS | viisumitietojärjestelmä |
| VRD | ajoneuvorekisteritiedot |

## LIITE 2: RAJATURVALLISUUDEN JA LAINVALVONNAN ALALLA KÄYTETTÄVÄT TIETOJÄRJESTELMÄT

### 1. Schengenin tietojärjestelmä (SIS)

SIS on muuttoliikkeen ja lainvalvonnan alalla suurin ja eniten käytetty tiedonvaihtojärjestelmä. Tämä keskitetty järjestelmä on käytössä 25 EU:n jäsenvaltiossa[29] ja neljässä Schengenin säännöstöön osallistuvassa maassa[30]. Järjestelmässä on nyt 63 miljoonaa kuulutusta. Kuulutuksia tekevät ja käsittelevät toimivaltaiset viranomaiset, kuten poliisi-, rajavalvonta- ja maahanmuuttoviranomaiset. Järjestelmässä on tiedot kolmansien maiden kansalaisista, joille on annettu maahantulokielto Schengen-alueelle, sekä kadonneista tai etsintäkuulutetuista EU:n ja kolmansien maiden kansalaisista (myös lapsista) ja etsityistä esineistä (aseet, ajoneuvot, henkilöasiakirjat, teollisuuslaitteistot ym.). SIS-järjestelmän erityispiirre muihin tietojenjakovälineisiin verrattuna on se, että sen tietoihin on liitetty ohjeet konkreettisista toimenpiteistä, jotka kentällä toimivien viranomaisten olisi toteutettava (esimerkiksi pidätys tai takavarikko).

SIS-tarkastus on pakollinen lyhytaikaisten viisumien käsittelyn ja kolmansien maiden kansalaisille tehtävien rajatarkastusten yhteydessä, ja se on tehtävä satunnaisesti[31] myös EU:n kansalaisille ja muille vapaan liikkuvuuden oikeuden piiriin kuuluville henkilöille. Lisäksi SIS-tarkastus olisi tehtävä automaattisesti kaikkien unionin sisällä tehtävien poliisitarkastusten yhteydessä.

### 2. Viisumitietojärjestelmä (VIS)

VIS on keskitetty järjestelmä, jossa jäsenvaltiot vaihtavat tietoja lyhytaikaista oleskelua varten myönnettävistä viisumeista. Siinä käsitellään tietoja ja päätöksiä, jotka koskevat hakemuksia lyhytaikaisen viisumin myöntämiseksi Schengen-alueella vierailua tai sen läpi tapahtuvaa kauttakulkua varten. Järjestelmässä ovat mukana kaikki Schengen-maiden konsulaatit (noin 2 000) ja kaikki niiden ulkorajojen ylityspaikat (yhteensä noin 1 800).

VIS sisältää tiedot viisumihakemuksista ja niitä koskevista päätöksistä sekä myönnettyjen viisumien mahdollisesta kumoamisesta, mitätöinnistä tai pidentämisestä. Tällä hetkellä järjestelmässä on tiedot 20 miljoonasta viisumihakemuksesta, ja siinä voidaan käsitellä yli 50 000 hakua tunnissa. Jokaisen viisuminhakijan on annettava järjestelmään yksityiskohtaiset henkilötiedot, digitaalinen valokuva ja kymmenen sormenjälkeä. VIS on tehokas keino tarkistaa viisuminhakijoiden henkilöllisyys, arvioida sääntöjenvastaiseen maahantuloon mahdollisesti liittyviä tapauksia ja turvallisuusriskejä sekä estää viisumikeinottelu.

VIS-järjestelmästä tarkistetaan rajanylityspaikoilla tai jäsenvaltioiden alueella viisuminhaltijoiden henkilöllisyys vertaamalla heidän sormenjälkiään järjestelmään tallennettuihin tietoihin. Näin voidaan varmistaa, että viisumia hakenut henkilö on sama kuin se, joka ylittää rajan. VIS-järjestelmässä tehtävän sormenjälkihaun avulla voidaan myös tunnistaa henkilö, jolla ei kenties ole henkilöasiakirjoja, jos hän on hakenut viisumia viiden edeltävän vuoden aikana.

---

[29] Kaikki paitsi Irlanti, Kypros ja Kroatia.

[30] Sveitsi, Liechtenstein, Norja, Islanti.

[31] Tätä sääntöä on tarkoitus muuttaa, ks. komission ehdotus COM/2015/0670 Schengenin rajasäännöstön muuttamisesta.

## 3. EURODAC

Eurodac-järjestelmä (European Dactyloscopy) sisältää turvapaikanhakijoiden ja Schengen-alueen ulkorajat sääntöjenvastaisesti ylittäneiden kolmansien maiden kansalaisten sormenjälkitiedot. Järjestelmän ensisijaisena tarkoituksena on määrittää, mikä EU:n jäsenvaltio on Dublin-asetuksen mukaisesti vastuussa turvapaikkahakemuksen käsittelystä. Järjestelmä on käytössä rajanylityspaikoilla, mutta se ei ole rajaturvallisuusjärjestelmä, toisin kuin SIS ja VIS.

EU:n alueelle sääntöjenvastaisesti tulevilta henkilöiltä otetaan sormenjäljet rajanylityspaikalla. Ne tallennetaan Eurodac-järjestelmään, jotta tulijan henkilöllisyys voidaan tarkistaa, jos hän hakee myöhemmin turvapaikkaa. Maahanmuutto- ja poliisiviranomaiset voivat myös vertailla järjestelmässä EU:n jäsenvaltioiden alueella sääntöjenvastaisesti oleskelevien henkilöiden sormenjälkiä tarkistaakseen, ovatko nämä hakeneet turvapaikkaa toisessa jäsenvaltiossa. Myös lainvalvontaviranomaisilla ja Europolilla on oikeus tehdä hakuja Eurodac-järjestelmässä vakavien rikosten ja terrorismirikosten ehkäisemistä, paljastamista ja tutkintaa varten.

Kun turvapaikanhakijoiden ja EU:n alueelle sääntöjenvastaisesti tulleiden henkilöiden sormenjäljet tallennetaan keskitettyyn järjestelmään, heidän edelleen liikkumistaan[32] EU:n sisällä voidaan selvittää ja seurata kansainvälistä suojelua koskevan hakemuksen tai palauttamispäätöksen tekemiseen asti (tulevaisuudessa voidaan tehdä vastaava SIS-kuulutus). EU:n alueella sääntöjenvastaisesti oleskelevien henkilöiden valvonta ja heidän henkilöllisyytensä selvittäminen on tarpeen, jotta viranomaiset voivat hankkia heille palauttamista varten tarvittavat asiakirjat heidän lähtömaastaan.

## 4. Varastettuja ja kadonneita matkustusasiakirjoja koskeva tietokanta (SLTD)

Varastettuja ja kadonneita matkustusasiakirjoja koskevaan keskitettyyn Interpolin tietokantaan (SLTD) kootaan tiedot varastetuista ja kadonneista passeista ja muista matkustusasiakirjoista viranomaisten Interpolille tekemien ilmoitusten perusteella. Tietokannassa on tiedot myös varastetuista passilomakkeista. Tiedot varastetuista ja kadonneista matkustusasiakirjoista, joista on tehty ilmoitus SIS-järjestelmään osallistuvien maiden viranomaisille, tallennetaan sekä SLTD-tietokantaan että SIS-järjestelmään. SLTD sisältää tiedot myös sellaisista matkustusasiakirjoista, joista ovat tehneet ilmoituksen SIS-järjestelmän ulkopuoliset maat (Irlanti, Kroatia, Kypros ja kolmannet maat).

Kuten 9. ja 20. marraskuuta 2015 annetuissa neuvoston päätelmissä ja Schengenin säännöstön kohdennetusta muuttamisesta 15. joulukuuta 2015 tehdyssä komission asetusehdotuksessa[33] todetaan, kaikkien kolmansien maiden kansalaisten ja vapaan liikkumisoikeuden piiriin kuuluvien henkilöiden matkustusasiakirjat olisi tarkistettava SLTD-tietokannassa. Kaikilla rajatarkastusasemilla on oltava yhteys SLTD-tietokantaan. Lisäksi turvallisuutta voitaisiin parantaa tekemällä SLTD-hakuja myös Schengen-alueen sisällä tehtävissä lainvalvontatarkastuksissa.

[32] Esimerkiksi Kreikkaan saapuvat pakolaiset, jotka eivät edes harkitse turvapaikan hakemista Kreikasta, vaan siirtyvät edelleen maitse muihin jäsenvaltioihin.

[33] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EY) N:o 562/2006 muuttamisesta siltä osin kuin on kyse tietokantojen käyttöön perustuvien tarkastusten vahvistamisesta ulkorajoilla, COM(2015) 670 final.

## 5. Matkustajien ennakkotiedot (API)

Matkustajien ennakkotietojen avulla selvitetään matkustajien henkilöllisyys ennen kuin nämä nousevat EU:hun saapuville lennoille ja EU:hun sääntöjenvastaisesti tulevien henkilöiden henkilöllisyys näiden saapuessa. Ennakkotiedot muodostuvat matkustusasiakirjassa olevista tiedoista, joista käyvät ilmi matkustajan koko nimi, syntymäaika, kansalaisuus ja matkustusasiakirjan tyyppi ja numero. Lisäksi saadaan tiedot lähtöpaikasta ja rajanylityspaikasta, jonka kautta matkustaja saapuu EU:n alueelle, ja muita matkaan liittyviä tietoja. Matkustajan ennakkotiedot kerätään yleensä lähtöselvityksen yhteydessä.

Meriteitse saapuvista matkustajista on toimitettava ennakkotiedot Kansainvälisen meriliikenteen helpottamista koskevan yleissopimuksen mukaisesti 24 tuntia ennen aluksen aikataulun mukaista saapumisaikaa. Direktiivissä 2010/65/EU[34] säädetään, että tiedot on toimitettava SafeSeaNet-järjestelmän, sähköisen tullijärjestelmän ja muut sähköiset järjestelmät yhdistävän keskitetyn sähköisen palvelupisteen kautta.

Matkustajien ennakkotietojen tallentamista varten ei ole olemassa keskitettyä EU:n järjestelmää.

## 6. Europolin tietojärjestelmä

Europolin tietojärjestelmä (EIS) on keskitetty rikostietokanta tutkintatarkoituksia varten. Jäsenvaltiot ja Europol voivat käyttää sitä vakavaa rikollisuutta ja terrorismia koskevien tietojen tallentamiseen ja hakemiseen. Tiedot koskevat henkilöitä, henkilöasiakirjoja, ajoneuvoja, aseita, puhelinnumeroita, sähköpostiosoitteita, sormenjälkiä, DNA-tietoja ja verkkorikollisuuteen liittyviä tietoja, jotka voidaan yhdistää toisiinsa eri tavoin niin, että voidaan saada tarkempi ja jäsennellympi kuva tietystä rikostapauksesta. EIS-järjestelmä tukee lainvalvontayhteistyötä. Se ei ole rajavalvontaviranomaisten käytettävissä.

Tietojenvaihto tapahtuu SIENA[35]-alustalla. Se on suojattu tietoliikenneverkko, joka yhdistää toisiinsa Europolin päätoimiston ja sen yhdyshenkilötoimistot, Europolin kansalliset yksiköt, tätä varten nimetyt toimivaltaiset viranomaiset (mm. tulli ja varallisuuden takaisin hankinnasta vastaavat toimistot) sekä järjestelmään osallistuvat kolmannet osapuolet.

Toukokuussa 2017 ryhdytään soveltamaan Europolin uutta oikeudellista kehystä. Se antaa Europolille entistä paremmat operatiiviset valmiudet tehdä analyyseja ja tunnistaa saatavilla oleviin tietoihin sisältyviä yhteyksiä.

## 7. Prüm-puitteet

Prüm-puitteet perustuvat jäsenvaltioiden välillä tehtyyn monenväliseen sopimukseen[36], jonka nojalla vaihdetaan DNA- ja sormenjälkitietoja sekä ajoneuvojen rekisteröintitietoja. Tietojenvaihto tapahtuu siten, että kaikki EU:n jäsenvaltioiden kansalliset järjestelmät on liitetty toisiinsa niin, että niissä voidaan tehdä hakuja kaikkiin järjestelmiin. Jos haku tuottaa tulokseksi osuman jonkin toisen jäsenvaltion tietokannassa, tarkemmat tiedot vaihdetaan kahdenvälisen mekanismin puitteissa.

---

[34] Euroopan parlamentin ja neuvoston direktiivi 2010/65/EU, annettu 20 päivänä lokakuuta 2010, jäsenvaltioiden satamiin saapuvia ja/tai satamista lähteviä aluksia koskevista ilmoitusmuodollisuuksista ja direktiivin 2002/6/EY kumoamisesta.

[35] Secure Information Exchange Network Application.

[36] Vuonna 2005 tehty Prümin sopimus. Sopimus on otettu osaksi EU:n säännöstöä vuonna 2008 neuvoston päätöksellä 2008/615/YOS.

## 8. Eurooppalainen rikosrekisteritietojärjestelmä (ECRIS)

ECRIS on sähköinen tiedonvaihtojärjestelmä, jossa vaihdetaan tietoja tietylle henkilölle EU:n jäsenvaltioissa annetuista aiemmista rikostuomioista kyseistä henkilöä koskevan uuden rikosoikeudenkäynnin yhteydessä. Kansallisen lainsäädännön niin salliessa tietoja voidaan vaihtaa myös muuta tarkoitusta varten. Tuomiojäsenvaltioiden on ilmoitettava toisten jäsenvaltioiden kansalaisille annetuista tuomioista näiden kansalaisuusjäsenvaltiolle. Kansalaisuusjäsenvaltio tallentaa nämä tiedot, jotta se voi tarvittaessa toimittaa kansalaisistaan ajantasaiset rikosrekisteritiedot riippumatta siitä, missä EU:n jäsenvaltiossa tuomio on annettu.

Järjestelmässä on mahdollista vaihtaa tietoja myös kolmansien maiden kansalaisille ja kansalaisuudettomille henkilöille annetuista rikostuomioista. Kussakin jäsenvaltiossa on nimetty keskusviranomainen, joka toimii ECRIS-verkoston yhteyspisteenä ja hoitaa kaikki siihen liittyvät tehtävät, kuten ilmoitusten toimittamisen, rikosrekisteritietojen tallentamisen sekä tietopyyntöjen toimittamisen ja niihin vastaamisen.