

Bryssel den 6.4.2016  
COM(2016) 205 final

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH  
RÅDET**

**Starkare och smartare informationssystem för gränser och säkerhet**

## 1. INLEDNING

Europa är ett mobilt samhälle. Miljontals EU-medborgare och tredjelandsmedborgare passerar de inre och yttre gränserna varje dag. Under 2015 besökte fler än 50 miljoner tredjelandsmedborgare EU, vilket innebär mer än 200 miljoner gränspassager vid Schengenområdets yttre gränser.

Utöver dessa reguljära reseflöden orsakade konflikten i Syrien och andra kriser i världen 1,8 miljoner irreguljära gränspassager vid EU:s yttre gränser bara under 2015. EU-medborgarna förväntar sig att gränskontrollerna av personer vid de yttre gränserna ska vara effektiva, för att möjliggöra en effektiv migrationshantering och bidra till den inre säkerheten. Terroristattacker i Paris 2015 och i Bryssel i mars 2016 visade alltför tydligt att EU:s inre säkerhet konstant befinner sig under hot.

Dessa båda aspekter har belyst behovet av att gå samman och stärka EU:s gränsförvaltning, samarbetsramar för migration och säkerhet samt informationsverktyg på ett heltäckande sätt. Gränsförvaltning, brottsbekämpning och migrationskontroll är dynamiskt sammankopplade. Det är ett känt faktum att EU-medborgare har korsat den yttre gränsen för att resa till konfliktområden i terrorismsyfte och de kan utgöra ett hot när de återvänder. Terrorister har bevisligen använt irreguljära migrantrutter för att ta sig in i EU och sedan kunnat röra sig inom Schengenområdet utan att bli upptäckta.

Den europeiska säkerhetsagendan och den europeiska migrationsagendan har angett riktningen för utveckling och genomförande av EU-politiken för att ta itu med de parallella utmaningarna med migrationshantering samt kampen mot terrorism och organiserad brottslighet. Detta meddelande bygger på synergier mellan dessa två agendor och är avsett att vara en startpunkt för en diskussion om hur befintliga och framtida informationssystem skulle kunna förbättra både förvaltningen av de yttre gränserna och EU:s inre säkerhet. Det kompletterar förslaget från december 2015 om att inrätta en europeisk gräns- och kustbevakningsbyrå och förbättra krisförebyggande och krisinsatser vid de yttre gränserna.

På EU-nivå finns det ett flertal informationssystem som tillhandahåller gränskontrolltjänstemän och poliser relevant information om personer, men EU:s uppgiftshanteringsstruktur är inte perfekt. I detta meddelande framläggs några möjliga sätt att maximera nyttan av de befintliga informationssystemen och vid behov utveckla nya och kompletterande åtgärder för att åtgärda luckor. I meddelandet poängteras också behovet av att förbättra interoperabiliteten mellan informationssystemen på lång sikt, vilket även Europeiska rådet och rådet har framhållit<sup>1</sup>. Det läggs fram idéer om hur informationssystem kan utvecklas framöver för att säkra att gränskontrolltjänstemän, tullmyndigheter, poliser och rättsliga myndigheter har tillgång till den information de behöver.

Alla eventuella framtida initiativ ska utarbetas på grundval av principerna för bättre lagstiftning med ett offentligt samråd och en konsekvensbedömning, även när det gäller grundläggande rättigheter och speciellt rätten till skydd av personuppgifter.

---

<sup>1</sup> Europeiska rådets slutsatser av den 17–18 december 2015, gemensamt uttalande från EU:s ministrar med ansvar för rättsliga och inrikes frågor och företrädare för EU-institutionerna om terrorattacker i Bryssel den 22 mars 2016 (den 24 mars 2016), slutsatser från Europeiska unionens råd och medlemsstaterna, församlade i rådet, om terrorismbekämpning (den 20 november 2015).

## 2. UTMANINGAR

Avsaknaden av inre gränser inom Schengenområdet kräver en stark och tillförlitlig förvaltning av personers rörlighet över de yttre gränserna. Detta är en förutsättning för att garantera en hög inre säkerhet och fri rörlighet för personer inom det området. Samtidigt innebär avsaknaden av inre gränser att brottsbekämpande myndigheter i medlemsstaterna också har tillgång till relevanta personuppgifter. Det finns ett flertal informationssystem och databaser på EU-nivå som tillhandahåller gränskontrolltjänstemän, poliser och andra myndigheter personuppgifter som är relevanta för deras respektive behov<sup>2</sup>.

Informationssystemen har emellertid också brister som hindrar dessa nationella myndigheters arbete. Ett bättre informationsutbyte framhövdes därför som en nyckelprioritering i den europeiska säkerhetsagendan. De huvudsakliga bristerna är a) undermåliga funktioner i befintliga informationssystem, b) luckor i EU:s uppgiftshanteringsstruktur, c) ett komplicerat landskap av informationssystem som administreras på olika sätt och d) en splittrad uppgiftshanteringsstruktur för gränskontroll och säkerhet.

De befintliga informationssystemen för gränsförvaltning och inre säkerhet inom EU uppfyller många olika funktioner. Det finns dock ändå **brister i de befintliga systemens funktioner**. Om man betraktar de gränskontrollförfaranden som tillämpas för olika kategorier av resande är det tydligt att det finns brister både i vissa av dessa förfaranden och mellan de olika informationssystem som används för gränskontroller. De befintliga brottsbekämpningsverktygens prestanda bör likaledes optimeras. Därför bör åtgärder för att förbättra befintliga informationssystem övervägas (avsnitt 5).

Dessutom finns det **luckor i EU:s uppgiftshanteringsstruktur**. Problem återstår för gränskontroll av specifika kategorier av resande, såsom tredjelandsmedborgare som innehar en visering för längre vistelse. Det finns också en informationslucka före ankomst vid gränsen för de tredjelandsmedborgare som är befriade från viseringskravet. Det bör övervägas huruvida det finns ett behov av att åtgärda dessa luckor genom att vid behov utveckla ytterligare informationssystem (avsnitt 6).

Gränskontrolltjänstemän och speciellt poliser står inför ett **komplicerat landskap av informationssystem som administreras på olika sätt** på EU-nivå. Denna komplexitet skapar praktiska svårigheter speciellt vad gäller vilken databas som ska användas i en viss situation. Dessutom är inte alla medlemsstater uppkopplade till alla befintliga system<sup>3</sup>. Den nuvarande svårigheten med att komma åt informationssystem på EU-nivå skulle kunna minskas genom att det inrättas ett gemensamt sökgränssnitt på nationell nivå där de olika syftena för åtkomst iaktas (avsnitt 7.1).

EU:s befintliga uppgiftshanteringsstruktur för gränskontroll och säkerhet präglas av **splittring**. Orsaken till detta är att systemen har utvecklats i olika institutionella, rättsliga och politiska sammanhang. Information lagras separat i olika system som sällan är sammankopplade. Databaserna är inkonsekventa sinsemellan och de berörda myndigheterna har olika åtkomst till uppgifter. Detta kan leda till bristande insyn speciellt för brottsbekämpande myndigheter eftersom det kan vara väldigt svårt att se samband mellan olika uppgiftsfragment. Det är därför nödvändigt och brådskande att sträva efter integrerade lösningar för en förbättrad åtkomst till uppgifter för gränsförvaltning och säkerhet, i full överensstämmelse med de grundläggande

---

<sup>2</sup> Informationssystemen för gräns och säkerhet beskrivs kort i avsnitt 4, och i närmare detalj i bilaga 2.

<sup>3</sup> Särskilda villkor gäller för Danmark enligt protokoll 22 och för Förenade Kungariket och Irland enligt protokoll 21 och 36, samt enligt respektive lands anslutningsakt.

rättigheterna. För detta ändamål bör ett förfarande som ska leda till interoperabilitet mellan befintliga informationssystem inledas (avsnitt 7).

### 3. GRUNDLÄGGANDE RÄTTIGHETER

En fullständig överensstämmelse med de grundläggande rättigheterna och bestämmelserna om uppgiftsskydd är en grundförutsättning för att ta itu med alla dessa utmaningar.

En överensstämmelse med de grundläggande rättigheterna kräver att tekniken och informationssystemen är välutformade och används på rätt sätt. Tekniken och informationssystemen kan hjälpa myndigheterna att skydda medborgarnas grundläggande rättigheter. Biometrisk teknik kan minska risken för identitetsförväxlingar, diskriminering och rasprofilering. Tekniken kan också vara till hjälp med att ta itu med skyddsriskerna för barn, såsom att barn försvinner eller blir offer för människohandel, förutsatt att den åtföljs av garantier om de grundläggande rättigheterna och skyddsåtgärder. Den kan minska risken för att människor grips och anhålls på felaktiga grunder. Den kan också bidra till att öka säkerheten för medborgare inom Schengenområdet eftersom den bidrar till kampen mot terrorism och grov brottslighet.

Storskaliga informationssystem medför också potentiella integritetsrisker som bör förutses och åtgärdas på lämpligt sätt. Insamling och användning av personuppgifter i dessa system har följder för rätten till integritet och skyddet av personuppgifter som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna. Alla system måste överensstämma med principerna om uppgiftsskydd och principerna om nödvändighet, proportionalitet, ändamålsbegränsning och uppgifternas kvalitet. Det måste finnas garantier för att säkra de registrerades rätt till skydd av privatliv och personuppgifter. Uppgifterna bör sparas endast så länge som det är nödvändigt för det syfte i vilket de insamlades. Mekanismer som säkerställer en korrekt riskbedömning och effektivt skydd av de registrerades rättigheter bör införas.

I december 2015 nådde medlagstiftarna en politisk överenskommelse om reformen av uppgiftsskydd. När den nya allmänna uppgiftsskyddsförordningen och uppgiftsskyddsdirektivet för polis och straffrättsliga myndigheter<sup>4</sup> har antagits och blir tillämpliga 2018 kommer de att utgöra en harmoniserad ram för behandling av personuppgifter.

Ändamålsbegränsning är en grundprincip för uppgiftsskydd som fastställs i stadgan om de grundläggande rättigheterna. På grund av de olika institutionella, rättsliga och politiska sammanhangen där de olika informationssystemen på EU-nivå har utvecklats genomfördes principen om ändamålsbegränsning genom en uppdelad uppgiftshanteringsstruktur<sup>5</sup>. Det här är en av orsakerna till att EU:s befintliga uppgiftshanteringsstruktur för gränskontroll och inre säkerhet är splittrad. När den nya övergripande ramen för uppgiftsskydd i EU är i kraft och med hjälp av betydelsefull utveckling inom teknik och it-säkerhet kan principen om ändamålsbegränsning lättare tillämpas på åtkomst till och användning av lagrade uppgifter, i full överensstämmelse med stadgan om de grundläggande rättigheterna och med EU-domstolens aktuella rättspraxis. Garantier såsom uppdelning av uppgifter inom ett system och särskilda regler för tillgång och användning för varje uppgiftskategori och användare bör säkerställa den nödvändiga ändamålsbegränsningen i integrerade lösningar för uppgiftshantering. Detta

---

<sup>4</sup> Se [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm).

<sup>5</sup> COM(2010) 385 final.

bereder väg för interoperabilitet mellan informationssystem som åtföljs av de nödvändiga strikta reglerna om åtkomst och användning utan att den befintliga ändamålsbegränsningen påverkas.

Ett inbyggt uppgiftsskydd och uppgiftsskydd som standard är nu principer i EU:s uppgiftsskyddsregler. Kommissionen strävar efter att följa dessa riktlinjer i arbetet med att utveckla nya verktyg som förlitar sig på användning av informationsteknik. Detta förutsätter att uppgiftsskyddet ska vara inbyggt i det föreslagna verktygets tekniska bas, och uppgiftsbehandlingen begränsas därmed till det som är nödvändigt för ett specifikt ändamål och enbart de enheter som har behovsenlig behörighet får åtkomst till uppgifterna<sup>6</sup>.

Kraven i stadgan om de grundläggande rättigheterna och särskilt de nya reformverktygen för uppgiftsskydd kommer att vägleda kommissionen i arbetet med att åtgärda de nuvarande luckorna och bristerna i EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet. Detta säkerställer att den kommande utvecklingen av informationssystem på dessa områden följer de högsta standarderna för uppgiftsskydd, och att de respekterar och bidrar till de grundläggande rättigheterna i enlighet med stadgan om de grundläggande rättigheterna.

#### 4. ÖVERSIKT AV INFORMATIONSSYSTEM FÖR GRÄNSER OCH SÄKERHET<sup>7</sup>

EU:s befintliga informationssystem för gränsförvaltning och inre säkerhet har alla egna mål, syften, rättsliga grunder<sup>8</sup>, användargrupper och institutionella sammanhang. Tillsammans bildar de ett komplicerat nät av relevanta databaser.

De tre huvudsakliga **centraliserade informationssystem** som utvecklats av EU är i) Schengens informationssystem (SIS) med ett brett spektrum av registreringar om personer och föremål, ii) informationssystemet för viseringar (VIS) som innehåller uppgifter om viseringar för kortare vistelser och iii) Eurodacsystemet med fingeravtrycksuppgifter om asylsökande och tredjelandsmedborgare som har passerat de yttre gränserna på ett irreguljärt sätt. Dessa tre system kompletterar varandra och omfattar, med undantag för SIS, i första hand tredjelandsmedborgare. Systemen är också till stöd för de nationella myndigheterna i kampen mot brottslighet och terrorism<sup>9</sup>. Detta gäller speciellt SIS som är det informationsdelningsverktyg som används mest i dagens läge. Utbyte av information för dessa system sker via s-Testa<sup>10</sup>, en säker kommunikationsinfrastruktur som utvecklats specifikt för ändamålet.

---

<sup>6</sup> En omfattande beskrivning om principen om ”privacy by design” finns i yttrandet från Europeiska datatillsynsmannen om att främja förtroendet för informationssamhället genom ett stärkt data- och integritetsskydd, den 18 mars 2010.

<sup>7</sup> I bilaga 2 finns en förteckning över befintliga informationssystem för gränsförvaltning och brottsbekämpning.

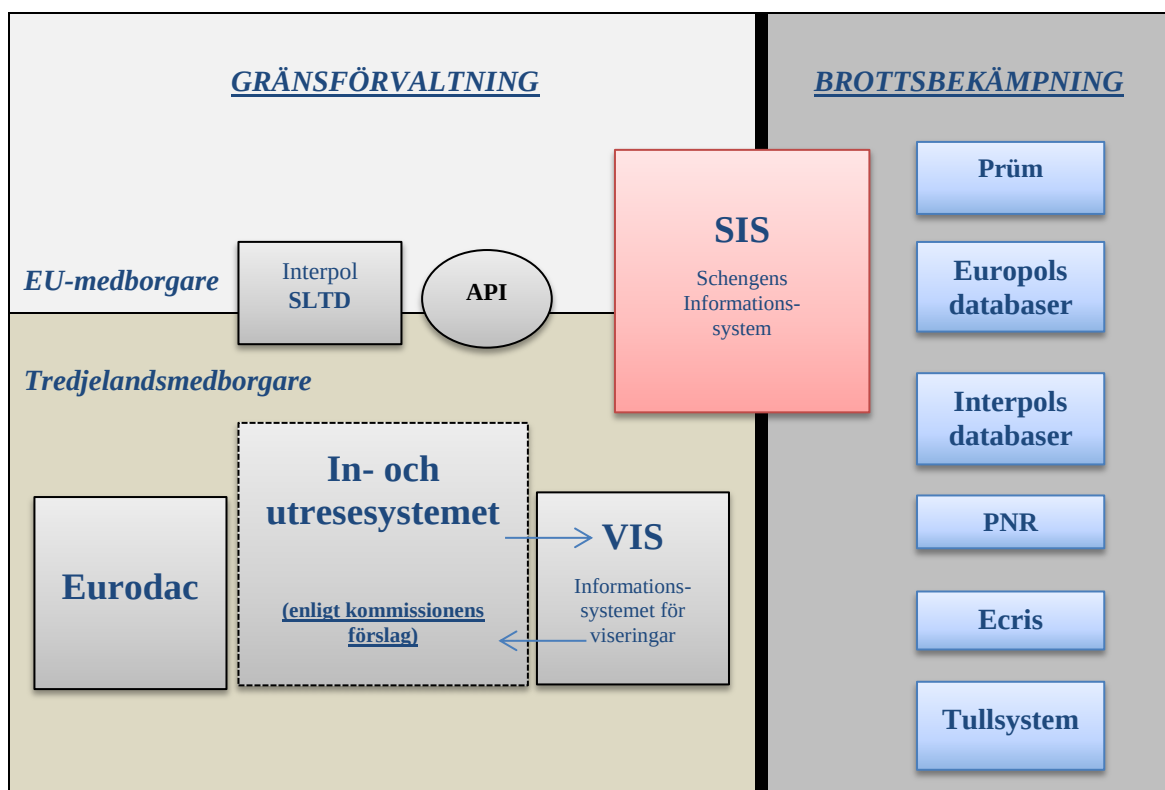
<sup>8</sup> Särskilda villkor gäller för Danmark enligt protokoll 22 och för Förenade Kungariket och Irland enligt protokoll 21 och 36.

<sup>9</sup> Brottsbekämpande myndigheter har en begränsad åtkomst till VIS och Eurodac eftersom brottsbekämpning är ett underordnat mål för dessa system. När det gäller VIS måste medlemsstaterna utse en myndighet som har ansvar för att kontrollera åtkomst i brottsbekämpningssyfte och poliser måste bestyrka att deras åtkomst är nödvändig för brottsundersökningar. För att få åtkomst till Eurodac måste den undersökande myndigheten först söka i det nationella Afis, Prüm och VIS.

<sup>10</sup> Ersätts inom kort av Testa-NG.

Utöver dessa befintliga system föreslår kommissionen att ett fjärde centraliserat gränsförvaltningssystem ska inrättas. **In- och utresesystemet** (EES)<sup>11</sup> förväntas ha genomförts senast 2020 och berör även det tredjelandsmedborgare.

**Diagram 1** En schematisk översikt av de huvudsakliga informationssystemen för gränsförvaltning och brottsbekämpning:



Ytterligare befintliga verktyg för gränsförvaltning är Interpols databas över stulna och förkomna resehandlingar (i diagrammet används den engelska förkortningen SLTD) och systemet för förhandsinformation om passagerare (API-uppgifter) på ankommande flygningar till EU. Dessa verktyg gäller både EU-medborgare och tredjelandsmedborgare.

EU har utvecklat **decentraliserade verktyg för informationsutbyte** speciellt för brottsbekämpning, brottsutredning och rättsligt samarbete, dvs. i) Prümramen för utbyte av DNA, fingeravtryck och fordonsregisteruppgifter och ii) det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris). Ecris möjliggör utbyte av uppgifter via ett säkert nätverk om tidigare fällande domar som brottmålsdomstolar inom Europeiska unionen har avkunnat mot en viss person. Begäranden baserar sig främst på alfanumeriska identitetsuppgifter även om det är möjligt att utbyta biometrisk uppgifter.

**Europol** stöder informationsutbytet mellan nationella polismyndigheter i egenskap av EU:s centrum för information om brottslighet. Europols informationssystem (EIS) är en centraliserad databas för information om brottslighet, där medlemsstaterna kan lagra och söka uppgifter om grov brottslighet och terrorism. Europols kontaktpunkter tillhandahåller ämnesinriktade analysregister med information om pågående operationer i medlemsstaterna. Europols nätapplikation för säkert informationsutbyte (Siena) gör det

<sup>11</sup> COM(2016) 194 final.

möjligt för medlemsstaterna att på ett enkelt, säkert och användarvänligt sätt utbyta information med varandra, med Europol eller med tredje parter som har ett samarbetsavtal med Europol. Samtidigt har Siena ett starkt fokus på interoperabilitet med andra system inom Europol, till exempel för att direkt utbyta uppgifter med kontaktpunkterna. Applikationen gör det möjligt att mata in den information som medlemsstaterna utbyter med varandra i Europol's databaser. Siena bör därför vara medlemsstaternas första val som kanal för att dela information om brottsbekämpning inom EU.

En annan uppsättning uppgiftshanteringssystem som ska utvecklas runtom i medlemsstaterna är systemet för **passageraruppgifter** (PNR-uppgifter)<sup>12</sup>. PNR-uppgifterna består av bokningsinformation som uppges vid bokning och incheckning.

Slutligen är också **tullmyndigheterna** viktiga aktörer inom samarbetet mellan olika organ vid de yttre gränserna. De har olika system<sup>13</sup> och databaser som innehåller information om förflyttning av varor, identifiering av ekonomiska aktörer och riskrelaterad information som kan användas för att stärka den inre säkerheten. Dessa system har också en egen kontrollerad, begränsad och säker infrastruktur (gemensamma kommunikationsnätet) som visat sig fungera bra. Det bör utredas närmare hur olika informationssystem för EU:s gränsförvaltning och tullaktioner och deras respektive infrastrukturer kan samverka och sammankopplas.

## 5. FÖRBÄTTRING AV BEFINTLIGA INFORMATIONSSYSTEM

De befintliga informationssystemen för gränsförvaltning och inre säkerhet inom EU uppfyller många olika funktioner. Systemen har emellertid fortfarande **brister** som bör åtgärdas för att deras prestanda ska kunna optimeras.

### *Schengens informationssystem (SIS)*

Gränskontroller mot **Schengens informationssystem** (SIS) sker för närvarande genom alfanumeriska sökningar (dvs. namn och födelsedatum). Fingeravtryck kan endast användas för att verifiera och bekräfta identiteten hos en person som redan har identifierats baserat på namnet. Denna säkerhetslucka gör det möjligt för personer som registrerats i SIS att undkomma en exakt match genom att använda förfälskade handlingar.

Denna allvarliga brist kommer att åtgärdas genom att man lägger till en fingeravtryckssökfunktion i SIS genom ett **automatiskt fingeravtrycksidentifieringssystem (Afis)**, som föreskrivs i den befintliga rättsliga ramen<sup>14</sup>. Afis bör vara i bruk senast i mitten av 2017<sup>15</sup>. Europol kommer att få åtkomst

---

<sup>12</sup> Se avsnitt 6.2.

<sup>13</sup> Tullinformationssystemen innefattar alla system som skapats enligt tullkodexen för gemenskapen (förordning (EEG) nr 2913/92) och den kommande tullkodexen för unionen (förordning (EU) nr 952/2013) samt beslutet om en papperslös miljö för tullen och handeln (beslut nr 70/2008/EG) och tullinformationssystemet som fastställdes i TIS-konventionen 1995. Syftet är att bistå i kampen mot tullrelaterad brottslighet genom att underlätta samarbetet mellan europeiska tullmyndigheter.

<sup>14</sup> Artikel 22 c i Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 381, 28.12.2006, s. 4) och rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

<sup>15</sup> I mars 2016 lade kommissionen fram en rapport till Europaparlamentet och rådet om tillgängligheten och driftklarheten för tekniken för identifiering av personer på grundval av fingeravtryck lagrade i andra generationen av Schengens informationssystem (SIS II).

till systemet när det har utvecklats och det kompletterar därmed Europol's system för brottsutredning och terrorismbekämpning, samt utbytet av fingeravtryck inom Prümramen. Kommissionen och eu-LISA kommer att utreda möjligheterna att använda det framtida Afis i sådana bredare syften.

På grundval av den pågående utvärderingen och en teknisk studie utreder kommissionen för närvarande **potentiella tilläggsfunktioner i SIS** med avsikt att lägga fram förslag till ändring av den rättsliga grunden för SIS. Följande aspekter övervägs:

- Införande av SIS-registreringar för irreguljära migranter vid beslut om återsändande.
- Användning av ansiktsbilder för biometrisk identifiering, utöver fingeravtryck.
- Automatisk informationsöverföring om en kontroll ger en träff.
- Lagring av information om träffar för diskreta och specifika kontrollregistreringar i SIS centraldatabas.
- Införande av en ny registreringskategori för "Efterlyst okänd person" för vilken kriminaltekniska uppgifter kan finnas i nationella databaser (t.ex. ett latent fingeravtryck som lämnats på en brottsplats)<sup>16</sup>.

Kommissionen kommer att fortsätta att använda EU-medel för att stödja genomförandet av projekt som gör det möjligt att söka samtidigt i SIS och Interpol's databas över stulna och förkomna resehandlingar, Interpol's databaser över efterlysta brottslingar respektive fordon och Interpol's register- och spårningssystem för olagliga vapen (iARMS), som är komplement till EU:s informationssystem<sup>17</sup>.

#### *Interpol's databas över stulna och förkomna resehandlingar*

Det är av yttersta vikt för en effektiv gränsförvaltning att alla tredjelandsmedborgares och EU-medborgares resehandlingar verifieras mot **Interpol's databas över stulna och förkomna resehandlingar**. Brottsbekämpande myndigheter bör också använda Interpol's databas över stulna och förkomna resehandlingar för sökningar inom Schengenområdet. Efter terroristattacker i Paris den 13 november 2015 efterlyste rådet elektronisk tillgång till Interpol's relevanta databaser vid samtliga yttre gränsövergångsställen och automatisk sökning på resehandlingar senast i mars 2016<sup>18</sup>. Alla medlemsstater bör inrätta de behövliga elektroniska förbindelserna och införa system som möjliggör automatisk uppdatering av uppgifter i Interpol's databas över stulna och förkomna resehandlingar.

#### *Förhandsinformation om passagerare (API)*

I enlighet med befintlig bästa praxis bör medlemsstaterna också öka mervärdet av **förhandsinformation om passagerare** (API-uppgifter) genom att införa en automatisk korskontroll av dessa uppgifter mot SIS och Interpol's databas över stulna och förkomna resehandlingar. Kommissionen kommer att utvärdera behovet av att revidera den rättsliga grunden för hantering av API-uppgifter för att säkerställa genomförande i en större utsträckning, och att inkludera en skyldighet för medlemsstaterna att kräva och använda API-uppgifter för alla ankommande och avgående flygningar. Detta är speciellt relevant

<sup>16</sup> Införandet av denna nya registrering ska utvärderas i syfte att eftersträva komplement till och undvika överlappning med den befintliga Prümramen för sökning av fingeravtryck i de nationella databaserna i EU:s medlemsstater.

<sup>17</sup> Syftet med de informationssökverktyg som utvecklats av Interpol, såsom en fast (Find) och en mobil (Mind) nätverksdatabas, är att underlätta samtidiga sökningar i Interpol's system och i SIS.

<sup>18</sup> Slutsatser från Europeiska unionens råd och medlemsstaterna, församlade i rådet, om terrorismbekämpning (20 november 2015).



sett till genomförandet av det framtida direktivet om passageraruppgifter eftersom en kombinerad användning av PNR-uppgifter och API-uppgifter ytterligare utökar PNR-uppgifternas verkan i kampen mot terrorism och grov brottslighet<sup>19</sup>.

#### *Informationssystemet för viseringar (VIS)*

Kommissionen genomför för närvarande också en allmän utvärdering av **informationssystemet för viseringar (VIS)**, vilken planeras vara klar under 2016. Utvärderingen fokuserar bland annat på hur VIS används för kontroller vid de yttre gränserna och inom medlemsstaternas territorium, och hur det bidrar till kampen mot identitets- och viseringsbedrägerier. På grundval av utvärderingen kommer kommissionen sedan att utreda möjligheterna att förbättra funktionerna i VIS genom bland annat följande:

- Förbättring av kvaliteten på ansiktsfoton för att möjliggöra biometrisk matchning.
- Användning av viseringssökandes biometriska uppgifter för att söka i det framtida automatiska fingeravtrycksidentifieringssystemet som ska utvecklas för SIS.
- Sänkning av åldersgränsen för att ta fingeravtryck av barn i åldrarna 6–12 år, dock med strikta garantier och skyddsåtgärder för de grundläggande rättigheterna<sup>20</sup>.
- Underlättad kontroll i Interpols databas över stulna och förkomna resehandlingar vid viseringsansökningar.

Medlemsstaterna utnyttjar möjligheterna till åtkomst till uppgifter i VIS i **brottsbekämpningssyfte** genom den befintliga rättsliga ramen i olika grad. I detta sammanhang har medlemsstater rapporterat om att brottsbekämpande myndigheter har praktiska problem med att få åtkomst till VIS. Genomförandet av åtkomst till Eurodac i brottsbekämpningssyfte är också fortfarande väldigt begränsat. Kommissionen kommer att utreda om det finns ett behov av att se över den rättsliga ramen för åtkomst till VIS och Eurodac i brottsbekämpningssyfte.

#### *Eurodac*

Såsom fastställs i meddelandet för en reform av det gemensamma asylsystemet och ökade möjligheter till laglig inresa till Europa<sup>21</sup> kommer kommissionen att lägga fram ett förslag till reform av **Eurodac** för att ytterligare förbättra dess funktioner gällande irreguljär migration och återsändande. Detta ska åtgärda en befintlig lucka i möjligheten att spåra irreguljära migranternas sekundära förflyttning mellan medlemsstaterna. Förslaget syftar dessutom till att effektivisera förfarandena för återsändande och återtagande genom att tillhandahålla verktyg för identifiering och utfärdande av nya resehandlingar för irreguljära migranter i återsändandesyfte. I detta sammanhang kommer förslaget också att omfatta informationsutbyte i Eurodac med tredjeländer, med iakttagande av erforderliga garantier om uppgiftsskydd.

#### *Europol*

EU har beviljat **Europol** åtkomst till de huvudsakliga centrala databaserna, men byrån har ännu inte utnyttjat denna möjlighet till fullo. Europol har rätt att komma åt och söka

<sup>19</sup> Mer information om det föreslagna direktivet om passageraruppgifter finns i avsnitt 6.2.

<sup>20</sup> Detta uppges vara tekniskt genomförbart i det gemensamma forskningscentrumets studie om identifiering av barns fingeravtryck, *Fingerprint Recognition for Children*, EUR 26193 EN, ISBN 978-92-79-33390-3 Children', 2013.

<sup>21</sup> COM(2016) 197 final.

direkt på uppgifter som lagrats i SIS för gripanden, diskreta och särskilda kontroller och beslagtagande av föremål. Hittills har Europol endast utfört ett relativt begränsat antal sökningar i SIS. Europol har haft laglig rätt till åtkomst till sökning i VIS sedan september 2013. Sedan juli 2015 tillåter Eurodacs rättsliga grund åtkomst för Europol. Byrån bör påskynda det pågående arbetet med att upprätta kopplingar till VIS och Eurodac. På ett mer allmänt plan kommer kommissionen att utvärdera behovet av att ge andra EU-byråer på området inrikes frågor utökad åtkomst till informationssystem, speciellt den framtida europeiska gräns- och kustbevakningsbyrån.

#### *Prümramen*

**Prümramen** utnyttjas för närvarande inte till sin fulla potential. Detta beror på att alla medlemsstater inte har genomfört sina rättsliga förpliktelser att integrera nätverket i sina egna system. Medlemsstaterna har mottagit betydande ekonomiskt och tekniskt stöd för genomförande av Prümramen och bör nu genomföra den till fullo. Kommissionen använder sig av de befogenheter som den har tilldelats för att säkerställa ett fullständigt genomförande av medlemsstaternas rättsliga förpliktelser och inledde en strukturerad dialog (via EU Pilot) med de berörda medlemsstaterna i januari 2016. Om medlemsstaternas svar inte är tillfredsställande kommer kommissionen utan tvekan att inleda överträdelseförfaranden.

#### *Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris)*

Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister, **Ecris**, gör det möjligt att utbyta uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer, men det finns inget fastställt förfaringsätt för att göra det på ett effektivt sätt. I januari 2016 antog kommissionen ett förslag till direktiv för att åtgärda denna lucka<sup>22</sup>. Där föreslog kommissionen att de nationella myndigheterna ska ges möjlighet att göra sökningar på tredjelandsmedborgare på grundval av fingeravtryck för säkrare identifiering. Europaparlamentet och rådet bör anta rättsakten under 2016.

#### *Övergripande frågor*

En allmän källa till oro vad gäller informationssystemen är medlemsstaternas **genomförandegrad**. Det ojämna genomförandet av Prümramen och avsaknaden av elektroniska kopplingar till Interpols databas över stulna och förkomna resehandlingar är två slående exempel på detta. För att förbättra informationssystemens genomförandegrad kommer kommissionen att noggrant övervaka varje medlemsstats framsteg<sup>23</sup>. Övervakningen kommer inte bara att gälla huruvida medlemsstaterna uppfyller sina rättsliga förpliktelser gällande informationssystem, utan även hur de tillämpar befintliga verktyg och om de följer bästa praxis. Kommissionen kommer att hämta information från olika källor för att granska och stödja genomförandegraden, däribland medlemsstaternas underrättelser och de besök som görs inom ramen för Schengenregelverkets utvärderings- och övervakningsmekanism.

Ett annat allmänt orosmoment gällande informationssystemen är **kvaliteten på införda uppgifter**. Om medlemsstaterna inte beaktar minimikvalitetskraven blir de lagrade uppgifternas tillförlitlighet och värde väldigt begränsat och risken för felaktiga matchningar och uteblivna träffar underminerar systemens värde. I syfte att förbättra kvaliteten på de uppgifter som införs ska eu-LISA utveckla en **central övervakningskapacitet för uppgiftskvalitet** för alla system de förvaltar.

---

<sup>22</sup> COM(2016) 7 final, 19.1.2016.

<sup>23</sup> Särskilda villkor gäller för Danmark enligt protokoll 22 och för Förenade Kungariket och Irland enligt protokoll 21 och 36.

De flesta informationssystem för gränsförvaltning och säkerhet hanterar uppgifter från rese- och identitetshandlingar. För att stärka gränserna och säkerheten behövs, förutom välfungerande system, ett lätt och säkert sätt att kontrollera rese- och identitetshandlingars autenticitet. I detta syfte kommer kommissionen att lägga fram åtgärder för att förbättra elektronisk **dokumentsäkerhet** och ID-hantering och för att stärka kampen mot förfälskade handlingar. De interoperabla dimensionerna av säker identifiering som kan uppnås genom förordningen om elektronisk identifiering<sup>24</sup> skulle kunna tillhandahålla sätt att genomföra detta.

### **Åtgärder för att förbättra befintliga informationssystem**

#### **Schengens informationssystem (SIS)**

- Kommissionen och eu-LISA ska utveckla och genomföra ett automatiskt fingeravtrycksidentifieringssystem i SIS senast i mitten av 2017.
- Kommissionen ska senast i slutet av 2016 lägga fram förslag på en reviderad rättslig grund för SIS för att förbättra dess funktioner ytterligare.
- Medlemsstaterna ska maximera sitt bruk av SIS, både genom att införa alla relevanta uppgifter och genom att använda sig av systemet då det behövs.

#### **Interpols databas över stulna och förkomna resehandlingar**

- Medlemsstaterna ska inrätta elektroniska förbindelser till Interpols verktyg vid alla yttre gränsövergångsställen.
- Medlemsstaterna ska iaktta sin skyldighet att införa och söka på uppgifter om stulna och förkomna resehandlingar i SIS och Interpols databas över stulna och förkomna resehandlingar samtidigt.

#### **Förhandsinformation om passagerare (API-uppgifter)**

- Medlemsstaterna ska automatisera användningen av API-uppgifter för kontroll mot SIS och Interpols databas över stulna och förkomna resehandlingar, i enlighet med befintlig bästa praxis.
- Kommissionen ska utvärdera behovet av att se över den rättsliga grunden för behandlingen av API-uppgifter.

#### **Informationssystemet för viseringar (VIS)**

- Kommissionen ska utreda hur VIS kan förbättras ytterligare före slutet av 2016.

#### **Eurodac**

- Kommissionen ska lägga fram ett förslag om att se över den rättsliga grunden för Eurodac för att ytterligare förbättra dess funktioner gällande irreguljär migration och återsändande.

#### **Europol**

- Europol ska till fullo utnyttja sina befintliga åtkomsträttigheter till sökningar i SIS, VIS och Eurodac.
- Kommissionen och Europol ska utreda och främja synergieffekter mellan Europolis informationssystem (EIS) och andra system, speciellt SIS.

<sup>24</sup> Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

- Kommissionen och eu-LISA ska utreda huruvida det automatiska fingeravtrycksidentifieringssystemet (Afis) som ska utvecklas för SIS även kan komplettera Europol's system för brottsutredning och terrorismbekämpning.

#### **Prümramen**

- Medlemsstaterna ska genomföra och använda Prümramen fullt ut.
- Vid behov ska kommissionen inleda överträdelseförfaranden mot de medlemsstater som inte är uppkopplade till Prümramen.
- Kommissionen och eu-LISA ska utreda huruvida det automatiska fingeravtrycksidentifieringssystem (Afis) som ska utvecklas för SIS även kan komplettera utbyte av uppgifter om fingeravtryck inom Prümramen.

#### **Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris)**

- Europaparlamentet och rådet ska 2016 anta lagförslaget om att ge nationella myndigheter rätt att göra sökningar på tredjelandsmedborgare i Ecris baserat på fingeravtryck.

#### **Övergripande frågor**

- Kommissionen ska **övervaka och främja informationssystemens genomförandegrad.**
- Eu-LISA ska utveckla **en central övervakningskapacitet för uppgiftskvalitet** för alla system de förvaltar.
- Kommissionen ska lägga fram åtgärder för att förbättra **elektronisk dokumentssäkerhet och ID-hantering** och för att förstärka kampen mot förfälskade handlingar.
- Kommissionen ska utreda hur olika informationssystem och deras respektive infrastrukturer för EU:s gränsförvaltning och **tullaktioner** kan samverka och sammankopplas.

## **6. UTVECKLING AV YTTERLIGARE INFORMATIONSSYSTEM OCH ÅTGÄRDANDE AV LUCKOR**

Även om befintliga informationssystem täcker ett väldigt brett spektrum av uppgifter som behövs inom gränsförvaltning och brottsbekämpning finns det också väsentliga luckor. Vissa av dessa luckor har kommissionen tagit ställning till genom lagstiftningsförslag, dvs. förslagen till ett in- och utresesystem och ett EU-system för passageraruppgifter. För de andra luckor som har identifierats bör en noggrann utvärdering göras av huruvida ytterligare EU-verktyg behövs.

### **1. In- och utresesystemet**

Kommissionen har parallellt med detta meddelande lagt fram reviderade lagstiftningsförslag om inrättande av ett in- och utresesystem. Efter att medlagstiftarna har antagit det är det upp till eu-LISA att utveckla och genomföra systemet i samarbete med Schengenmedlemsstaterna.

In- och utresesystemet kommer att omfatta uppgifter om gränspassage (in- och utresa) för alla tredjelandsmedborgare som besöker Schengenområdet för en kortare vistelse (högst 90 dagar under en 180-dagarsperiod), både resande som omfattas av viseringskravet och de som är befriade från viseringskravet, eller resande som stannar på grundval av den nya rundreseviseringen (upp till ett år). Målet med in- och utresesystemet är att a) förbättra

förvaltningen av de yttre gränserna, b) minska irreguljär migration genom att ta itu med fenomenet att personer stannar längre än tillåtet och c) bidra till kampen mot terrorism och grov brottslighet och på det sättet bidra till att säkerställa en hög nivå av inre säkerhet.

In- och utresesystemet kommer att användas för att registrera tredjelandsmedborgares identitet (alfanumeriska uppgifter, fyra fingeravtryck och ansiktsbild) samt uppgifter om deras resehandlingar, och koppla dessa till elektroniska uppgifter om in- och utresa. Den befintliga praxisen att stämpla resehandlingar kommer att avvecklas. In- och utresesystemet kommer att möjliggöra en effektiv förvaltning av tillåtna kortare vistelser, en ökad automatik vid gränskontroller och en förbättrad upptäckt av förfälskade handlingar och identitetsbedrägeri. Den centrala registreringen kommer att göra det möjligt att upptäcka personer som stannat längre än tillåtet och identifiera papperslösa personer inom Schengenområdet. Det föreslagna in- och utresesystemet fyller därmed en väsentlig lucka i landskapet med befintliga informationssystem.

## **2. Passageraruppgifter**

Passageraruppgifter (PNR-uppgifter) består av bokningsinformation med kontaktuppgifter, fullständiga uppgifter om resa och reservation, särskilda anmärkningar, plats- och bagageinformation samt betalningssätt. PNR-uppgifterna är behjälpliga och nödvändiga för att identifiera högriskresande i syfte att bekämpa terrorism, olaglig narkotikahandel, människohandel, sexuellt utnyttjande av barn och andra grova brott. Det föreslagna direktivet om passageraruppgifter kommer att garantera en bättre samverkan mellan nationella system och minska säkerhetsluckorna mellan medlemsstaterna. Det föreslagna direktivet om passageraruppgifter fyller därför en väsentlig lucka i tillgången till uppgifter som är nödvändiga för att bekämpa grov brottslighet och terrorism.

**Direktivet om passageraruppgifter bör antas och genomföras snarast möjligt.**

Det framtida direktivet föreskriver att medlemsstaterna måste inrätta enheter för passagerarinformation som tar emot PNR-uppgifter från lufttrafikföretagen. Något nytt centralt system eller någon ny databas kommer inte att skapas, utan genomförandet kunde ske genom ett visst mått av standardisering av nationella tekniska lösningar och förfaranden. Detta kommer att underlätta utbytet av PNR-uppgifter mellan enheterna för passagerarinformation i enlighet med det föreslagna direktivet. Kommissionen kommer därför att stödja medlemsstaternas analys av olika möjligheter att sammankoppla enheterna för passagerarinformation, i syfte att erbjuda standardiserade lösningar och förfaranden. När direktivet har antagits kommer kommissionen att påskynda arbetet med gemensamma protokoll och kompatibla dataformat för överföring av PNR-uppgifter från luftfartsföretag till enheterna för passagerarinformation. Kommissionen kommer att utarbeta ett utkast till genomförandeförordning inom tre månader efter att direktivet har antagits.

## **3. Informationslucka före ankomst för tredjelandsmedborgare som är befriade från viseringskravet**

Viseringsinnehavarnas identitets-, kontakt- och bakgrundsuppgifter registreras i VIS, medan den enda informationen om personer som är befriade från viseringskravet fås från deras resehandlingar. För resande som anländer luft- eller sjövägen kan dessa uppgifter kompletteras före ankomsten med API-uppgifter. Enligt det föreslagna direktivet om passageraruppgifter kommer deras PNR-uppgifter också att insamlas om de reser till EU med flyg. För personer som kommer in i EU via landgränserna finns ingen information tillgänglig innan ankomsten till EU:s yttre gräns.

Brottsbekämpande myndigheter kan få uppgifter om viseringsinnehavare från VIS om det är nödvändigt för att bekämpa grov brottslighet och terrorism, men för personer som är befriade från viseringskravet finns inga motsvarande uppgifter tillgängliga. Denna brist på information är speciellt beaktansvärd vad gäller förvaltningen av EU:s landgränser i en situation där avsevärda mängder resande som är befriade från viseringskravet anländer med bil, buss eller tåg. Flera av EU:s grannländer är redan befriade från viseringskravet och diskussioner om viseringsliberalisering framskrider mellan EU och andra grannländer. Detta kommer sannolikt att leda till en avsevärd ökning av resande som är befriade från viseringskravet inom en snar framtid.

Kommissionen kommer att utvärdera huruvida ett nytt EU-verktyg för att ta itu med detta problem är nödvändigt, genomförbart och proportionellt. Ett alternativ som kunde övervägas är ett **EU-system för reseuppgifter och resetillstånd** (Etias) där resande som är befriade från viseringskravet skulle registrera relevanta uppgifter om sin planerade resa. Den automatiska behandlingen av de här uppgifterna skulle kunna hjälpa gränskontrolltjänstemän vid deras bedömning av tredjelandsmedborgare som anländer för en kortare vistelse. Länder som Förenta staterna, Kanada och Australien har redan tagit i bruk motsvarande system, även för EU-medborgare.

Systemen för resetillstånd baserar sig på internetapplikationer där den sökande anger uppgifter om sin identitet, kontaktuppgifter, resans syfte, resplan osv. före avresan. Då den resande fått sitt tillstånd blir gränsförfarandena vid ankomsten snabbare och smidigare. Ett system som Etias skulle därmed också vara ett verktyg som underlättar resandet, utöver fördelarna för säkerheten och gränsförvaltningen och den potentiella användningen vid ömsesidighet i fråga om viseringar.

#### **4. Ett europeiskt polisregisterindex (Epris)**

Som anges i den europeiska säkerhetsagendan är tillgången till befintliga polisuppgifter i realtid mellan medlemsstaterna ett område för framtida arbete gällande informationsutbyte. Kommissionen kommer att utvärdera nödvändigheten av, den tekniska genomförbarheten av och proportionaliteten för ett europeiskt polisregisterindex (Epris) som skulle underlätta en gränsöverskridande åtkomst till information som finns i nationella brottsbekämpningsdatabaser. I detta syfte stöder kommissionen med EU-medel ett pilotprojekt som genomförs av en grupp bestående av fem medlemsstater med avsikt att utarbeta metoder för automatiska gränsöverskridande sökningar i nationella register på en träff/ingen träff-basis<sup>25</sup>. Kommissionen kommer att beakta resultaten av projektet i sin utvärdering.

#### **Åtgärder för att utveckla ytterligare informationssystem och ta itu med informationsluckor**

##### **In- och utresesystemet**

- Europaparlamentet och rådet bör betrakta lagstiftningsförslagen om in- och utresesystemet som en fråga av högsta prioritet, med målet att förslagen antas senast i slutet av 2016.

<sup>25</sup> Målet med pilotprojektet om automatiskt utbyte av uppgifter är att skapa ett tekniskt system som genom ett register gör det möjligt att se om det finns uppgifter om en individ eller en brottsundersökning i en eller flera medlemsstaters kriminalregister. Det automatiska svaret på en sökning i registret skulle endast ange om det finns uppgifter eller inte, ett så kallat svar med "träff" eller "ingen träff". Om sökningen ger en träff skulle följande steg vara att begära ytterligare personuppgifter genom de vanliga polisiära samarbetskanalerna.

### **Passageraruppgifter (PNR-uppgifter)**

- Europaparlamentet och rådet bör anta direktivet om passageraruppgifter senast i april 2016.
- Medlemsstaterna bör efter antagandet genomföra direktivet om passageraruppgifter snarast möjligt.
- Kommissionen ska stödja utbytet av uppgifter mellan enheter för passagerarinformation genom standardiserade lösningar och förfaranden.
- Kommissionen ska utarbeta ett utkast till genomförandebeslut om gemensamma protokoll och kompatibla dataformat för överföring av PNR-uppgifter från luftfartsföretag till enheter för passagerarinformation inom tre månader efter antagandet av direktivet om passageraruppgifter.

### **Informationslucka före ankomst för tredjelandssmedborgare som är befriade från viseringskravet**

- Kommissionen ska under 2016 utvärdera nödvändigheten av, den tekniska genomförbarheten av och proportionaliteten för införandet av ett nytt EU-verktyg såsom EU-systemet för reseuppgifter och resetillstånd.

### **Ett europeiskt polisregisterindex (Epris)**

- Kommissionen ska under 2016 utvärdera nödvändigheten av, den tekniska genomförbarheten av och proportionaliteten för införandet av ett europeiskt polisregisterindex.

## **7. MOT INTEROPERABILITET MELLAN INFORMATIONSSYSTEM**

Interoperabilitet innebär informationssystemss kapacitet att utbyta uppgifter och dela information. Det går att särskilja **fyra dimensioner av interoperabilitet**, som alla har rättsliga<sup>26</sup>, tekniska och operativa problematiska aspekter, däribland uppgiftsskydd:

- Ett gemensamt sökgränssnitt för att söka i flera informationssystem samtidigt och att få fram kombinerade resultat på en enda skärm.
- Sammankoppling av informationssystem så att uppgifter som har registrerats i ett system automatiskt konsulteras av ett annat system.
- Upprättande av en gemensam biometrisk matchningstjänst som stöder olika informationssystem.
- En gemensam databas för olika informationssystem (kärnmodul).

För att inleda ett förfarande som syftar till interoperabilitet mellan informationssystem på EU-nivå kommer kommissionen att inrätta en **expertgrupp på hög nivå för informationssystem och interoperabilitet** med EU-organ, nationella experter och berörda parter från institutionerna. Expertgruppen får som uppdrag att beakta de rättsliga, tekniska och operativa aspekterna av de olika alternativen för att uppnå interoperabilitet mellan informationssystem, däribland de tillgängliga alternativens nödvändighet, tekniska genomförbarhet och proportionalitet och deras följder för uppgiftsskyddet. Den bör ta itu med de befintliga bristerna och kunskapsluckorna som orsakas av de europeiska informationssystemens komplexitet och splittring. Expertgruppen ska ha ett brett och omfattande perspektiv på gränsförvaltning och brottsbekämpning, och även beakta tullmyndigheternas roller, ansvarsområden och system i detta sammanhang. Gruppens

<sup>26</sup> Särskilda villkor gäller för Danmark enligt protokoll 22 och för Förenade Kungariket och Irland enligt protokoll 21 och 36.

arbetsmetod ska syfta till samverkan mellan alla relevanta erfarenheter, som tidigare alltför ofta har utvecklats var för sig.

Målet med det här förfarandet är att ta fram en övergripande strategisk vision för EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet, samt att föreslå lösningar för hur den ska genomföras.

Denna samrådsprocess ska **ha följande mål**:

- Informationssystemen bör komplettera varandra. Överlappningar bör undvikas och befintliga överlappningar bör avlägsnas. Luckor bör åtgärdas på lämpligt sätt.
- En modulär lösning bör eftersträvas, vilken utnyttjar den tekniska utvecklingen fullt ut och bygger på principen om *privacy by design*.
- Ett fullständigt iakttagande av alla grundläggande rättigheter för både EU-medborgare och tredjelandsmedborgare bör garanteras från första början, i enlighet med stadgan om de grundläggande rättigheterna.
- Informationssystemen bör vara sammankopplade och interoperabla, i den mån det är nödvändigt och genomförbart. Det bör bli lättare att söka samtidigt i flera system, för att garantera att all relevant information är tillgänglig för gränskontrolltjänstemän och poliser där och då detta är nödvändigt för deras respektive arbetsuppgifter, utan att ändra befintliga åtkomsträttigheter.

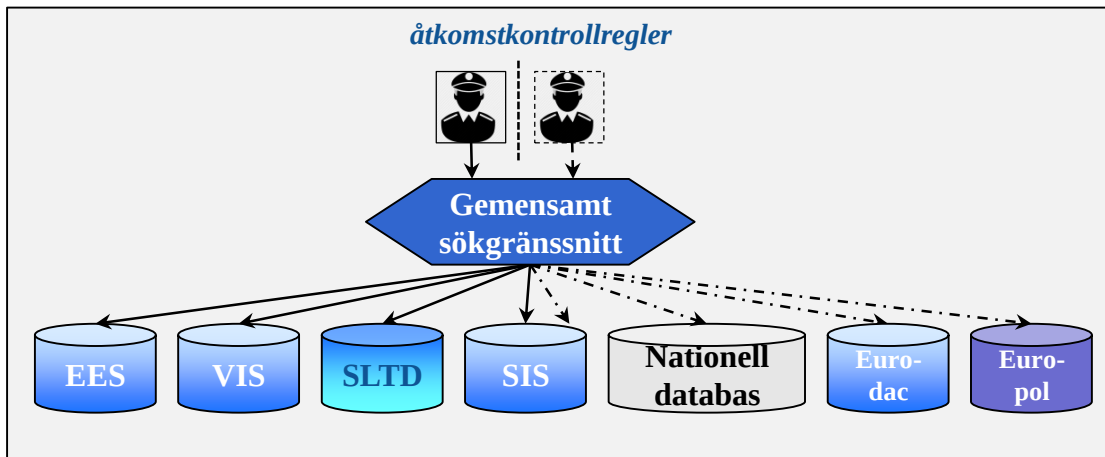
## **1. Gemensamt sökgränssnitt**

Den första dimensionen av interoperabilitet är **möjligheten att söka i flera informationssystem samtidigt, och att få fram kombinerade resultat på en enda skärm** för gränskontrolltjänstemän eller poliser, i fullständig enlighet med deras åtkomsträttigheter och respektive ändamål. Detta kräver plattformar med ett gemensamt sökgränssnitt som klarar av att söka i flera informationssystem samtidigt i en enda sökning. Genom att till exempel läsa av en resehandlings chip eller med hjälp av biometrisk uppgifter skulle denna plattform kunna göra sökningar i flera olika databaser samtidigt. Metoden med en gemensam sökning gäller alla myndigheter med ett behov av att komma åt och använda uppgifterna (dvs. gränskontrolltjänstemän, brottsbekämpande myndigheter och asyltjänstemän) i enlighet med ändamålsbegränsningen och strikta åtkomstkontrollregler. Det ska också kunna användas mobilt. Inrättandet av ett gemensamt sökgränssnitt minskar de europeiska informationssystemens komplexitet, eftersom det gör det möjligt för gränskontrolltjänstemän och poliser att göra sökningar i flera informationssystem samtidigt genom ett förfarande, och i enlighet med deras åtkomsträttigheter.

Flera medlemsstater har redan installerat sådana plattformar med ett gemensamt sökgränssnitt. Baserat på denna befintliga bästa praxis kommer kommissionen och eu-LISA tillsammans att arbeta för att fastställa en standardiserad lösning för ett gemensamt sökgränssnitt. Medlemsstaterna bör använda EU-medel inom ramen för de nationella programmen för fonden för inre säkerhet för att finansiera installationen av en sådan funktion. Kommissionen kommer att noggrant övervaka hur medlemsstaterna använder det gemensamma sökgränssnittet på nationell nivå.



**Diagram 2** Ett gemensamt sökgränssnitt



Det är lättare att göra en sökning i flera centraliserade eller nationella system (som på bilden) än att söka i decentraliserade system. Kommissionen och eu-LISA kommer att utreda om ett gemensamt sökgränssnitt också kan användas för att utföra samtidiga samservicesökningar i decentraliserade system som Prüm och Ecris. Kommissionen och eu-LISA kommer att göra denna utredning tillsammans med expertgruppen för informationssystem och interoperabilitet, utan att ändra befintliga åtkomsträttigheter.

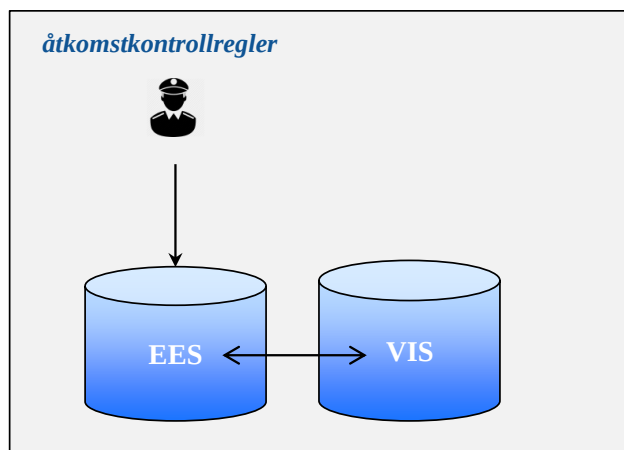
## 2. Sammankoppling av informationssystem

Den andra dimensionen av interoperabilitet är sammankoppling av informationssystem. Detta betyder att olika system och databaser rent tekniskt kan kommunicera sinsemellan. **Uppgifter som registreras i ett system skulle kunna konsulteras automatiskt av ett annat system på en central nivå.** Detta kräver en teknisk kompatibilitet mellan systemen, och de dataelement som lagras i dessa system (t.ex. fingeravtryck) bör vara driftskompatibla. En sammankoppling kan minska mängden uppgifter som cirkulerar på kommunikationsnätverk och överförs via nationella system.

En sammankoppling kräver lämpliga garantier för uppgiftsskydd och strikta åtkomstkontrollregler. Den politiska överenskommelse som lagstiftarna nådde i december 2015 om reformen av uppgiftsskyddet kommer att leda till införandet av en modern ram för uppgiftsskydd med dessa garantier i hela EU. Det är viktigt att medlagstiftarna antar den allmänna uppgiftsskyddsförordningen och uppgiftsskyddsdirektivet snarast möjligt.

Konceptet sammankoppling är inbyggt i det framtida in- och utresesystemet. Det framtida in- och utresesystemet ska kunna kommunicera direkt med VIS på central nivå och vice versa. Detta är ett viktigt steg i arbetet med att åtgärda den nuvarande splittringen i EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet samt relaterade problem. Den automatiska korskontrollen kommer att befria medlemsstaterna från behovet av att göra sökningar i VIS vid gränskontrollerna, minska underhållskraven och förbättra systemprestandan.

**Diagram 3** Sammankoppling av system: t.ex. in- och utresesystemet och VIS



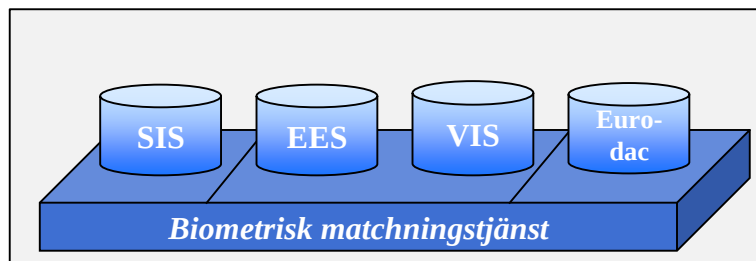
Nästa steg för kommissionen och eu-LISA är att analysera om sammankopplingen på central nivå mellan det framtida in- och utresesystemet och VIS kan utvidgas till SIS och om Eurodac och SIS kan kopplas samman. Kommissionen och eu-LISA kommer att göra denna analys tillsammans med expertgruppen för informationssystem och interoperabilitet.

### 3. En gemensam biometrisk matchningstjänst

En tredje dimension av interoperabilitet gäller biometriska kännetecken. När fingeravtryck tas med speciell utrustning på en medlemsstats konsulat är det till exempel av yttersta vikt att dessa avtryck kan matchas i VIS vid en annan medlemsstats gränsövergång där en annan typ av utrustning används. Samma krav gäller sökningar på fingeravtryck i andra system: biometriska prov bör uppfylla minimikraven på kvalitet och format för att denna typ av interoperabilitet utan svårigheter ska kunna uppnås.

På systemnivå möjliggör interoperabiliteten för biometriska kännetecken användningen av en gemensam biometrisk matchningstjänst för flera informationssystem, med iakttagande av reglerna för uppgiftsskydd genom att uppgifterna uppdelas i olika kategorier, med separata åtkomstkontrollregler för varje uppgiftskategori<sup>27</sup>. Sådana gemensamma tjänster ger avsevärda fördelar vad gäller ekonomi, underhåll och drift.

**Diagram 4** En gemensam biometrisk matchningstjänst



<sup>27</sup> Jämförbart med att dela en fysisk filserver med en stor mängd användare, som alla har specifika åtkomsträttigheter till enbart vissa mappar.

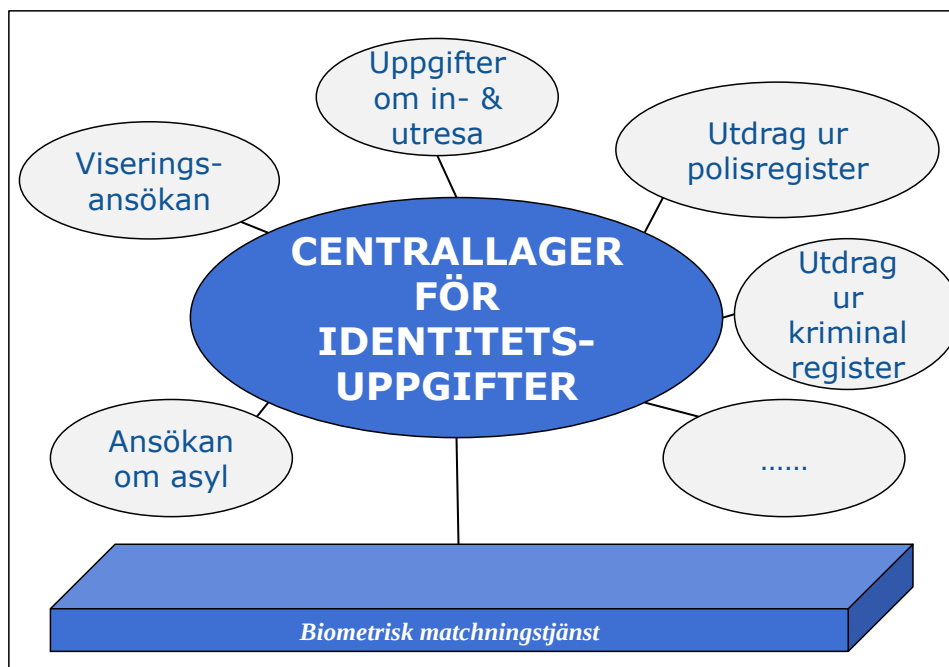
Kommissionen och eu-LISA kommer att analysera huruvida det är nödvändigt och tekniskt genomförbart att upprätta en gemensam biometrisk matchningstjänst för alla relevanta informationssystem. Kommissionen och eu-LISA kommer att göra denna analys tillsammans med expertgruppen för informationssystem och interoperabilitet.

#### 4. Ett gemensamt centrallager för databaser

Den mest ambitiösa strategin för interoperabilitet på lång sikt vore ett **gemensamt centrallager för databaser på EU-nivå för olika informationssystem**. Det gemensamma centrallagret skulle bestå av en kärnmodul som innehåller grundläggande uppgifter (alfanumeriska och biometriska uppgifter), medan de olika informationssystemens andra dataelement och specialegenskaper (t.ex. viseringsuppgifter) skulle lagras i specialmoduler. Kärnmodulen och specialmodulerna skulle vara sammankopplade för att länka respektive uppsättning uppgifter. Detta skulle skapa en **modulär och integrerad identitetshantering för gränser och säkerhet**. Överensstämmelsen med bestämmelserna om uppgiftsskydd skulle behöva garanteras, till exempel genom att uppdelat uppgifterna i olika kategorier, med separata åtkomstkontrollregler för varje uppgiftskategori.

Upprättandet av ett gemensamt centrallager för databaser skulle överbrygga den befintliga splittringen i EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet. Denna splittring strider mot principen om uppgiftsminimering, eftersom resultatet blir att samma uppgifter lagras flera gånger. Det gemensamma centrallagret skulle vid behov kunna göra det lättare att se samband och ge en överblick genom att kombinera enskilda dataelement som lagrats i olika informationssystem. Den skulle därmed fylla de befintliga kunskapsluckorna och belysa de områden där gränskontrolltjänstemän och poliser inte haft någon insyn.

**Diagram 5** Ett gemensamt centrallager för databaser



Alternativet att inrätta ett gemensamt centrallager för databaser på EU-nivå väcker väsentliga frågor om definitionen av ändamål, nödvändighet, teknisk genomförbarhet och proportionalitet för den uppgiftsbehandling som berörs. Det skulle kräva en fullständig revision av den rättsliga ram som inrättat de olika informationssystemen och det skulle

bara kunna vara ett mål på längre sikt. Expertgruppen för informationssystem och interoperabilitet kommer att beakta de rättsliga, tekniska och operativa frågor som förslaget om ett gemensamt centrallager väcker, däribland frågor om uppgiftsskydd.

Vad gäller alla fyra dimensioner av interoperabilitet som nämns ovan (ett gemensamt sökgränssnitt, sammankoppling av system, en gemensam biometrisk matchningstjänst och ett gemensamt centrallager) är det nödvändigt att de uppgifter som lagras i olika informationssystem eller moduler är kompatibla. För att uppnå detta är det viktigt att arbetet med **det universella meddelandeformatet** (UMF) framskrider så att det skapas en gemensam standard för alla relevanta informationssystem<sup>28</sup>.

### **Åtgärder för att uppnå interoperabilitet för informationssystem**

- Kommissionen ska inrätta en **expertgrupp för informationssystem och interoperabilitet** med EU:s organ, medlemsstater och berörda parter för att utreda de rättsliga, tekniska och operativa aspekterna av en förbättrad interoperabilitet mellan informationssystemen, däribland nödvändigheten av, den tekniska genomförbarheten av och proportionaliteten för tillgängliga alternativ och deras inverkan på uppgiftsskydd.

#### **Ett gemensamt sökgränssnitt**

- Kommissionen och eu-LISA ska stödja medlemsstaternas installation av ett gemensamt sökgränssnitt för sökning i centrala system.
- Kommissionen och eu-LISA ska, tillsammans med expertgruppen, utreda om gemensamma sökgränssnitt kunde användas för att utföra samservicesökningar samtidigt i alla relevanta system utan att ändra befintliga åtkomsträttigheter.

#### **Sammankoppling av informationssystem**

- Kommissionen och eu-LISA ska, tillsammans med expertgruppen, analysera om en sammankoppling mellan de centraliserade informationssystemen skulle kunna förbättras ytterligare, utöver den redan föreslagna sammankopplingen mellan in- och utresesystemet och informationssystemet för viseringar.

#### **En biometrisk matchningstjänst**

- Kommissionen och eu-LISA ska, tillsammans med expertgruppen, analysera nödvändigheten av och den tekniska genomförbarheten för inrättandet av en gemensam biometrisk matchningstjänst för alla relevanta informationssystem.

#### **Ett gemensamt centrallager för databaser (kärnmodul)**

- Kommissionen och eu-LISA ska, tillsammans med expertgruppen, utreda de rättsliga, tekniska, operativa och ekonomiska effekterna av att på lång sikt utveckla ett gemensamt centrallager.
- Kommissionen och eu-LISA ska delta i det pågående arbetet med ett globalt universellt meddelandeformat för alla relevanta informationssystem.

<sup>28</sup> Kommissionen har understött den pågående utvecklingen av det universella meddelandeformatet i meddelandet om den europeiska modellen för informationsutbyte (EIXM) från 2012 och finansierar för närvarande det tredje pilotprojektet för det universella meddelandeformatet. Syftet är att skapa en gemensam standard för alla relevanta databaser, vilken kan användas på nationell nivå (medlemsstaterna), EU-nivå (de centrala systemen och organen) och internationell nivå (Interpol).

## 8. SLUTSATS

Detta meddelande är inledningen på en diskussion om hur EU:s informationssystem bättre kan förstärka gränsförvaltningen och den inre säkerheten, på grundval av avsevärda synergier mellan den europeiska säkerhetsagendan och den europeiska migrationsagendan. Ett flertal informationssystem förser redan nu gränskontrolltjänstemän och poliser med relevant information, men dessa system är inte perfekta. EU står inför utmaningen att bygga en starkare och smartare uppgiftshanteringsstruktur, i full överensstämmelse med de grundläggande rättigheterna, speciellt skyddet av personuppgifter och principen om ändamålsbegränsning.

Luckorna i EU:s uppgiftshanteringsstruktur bör åtgärdas. Tillsammans med detta meddelande har kommissionen lagt fram ett förslag till ett in- och utresesystem vilket bör antas snarast möjligt. Direktivet om passageraruppgifter bör också antas inom de närmaste veckorna. Förslaget om en europeisk gräns- och kustbevakning bör antas före sommaren. Parallellt med dessa kommer kommissionen att fortsätta arbeta för att stärka och vid behov strama upp befintliga system, till exempel genom att utveckla ett automatiskt fingeravtrycksidentifieringssystem för Schengens informationssystem.

Medlemsstaterna bör utnyttja de befintliga informationssystemen fullt ut och inrätta de nödvändiga tekniska förbindelserna till alla informationssystem och databaser, i enlighet med deras rättsliga förpliktelser. Befintliga brister, speciellt inom Prümramen, bör åtgärdas snarast möjligt. Detta meddelande inleder en diskussion och ett förfarande för att åtgärda luckor och brister i systemen, men det är upp till medlemsstaterna att skyndsamt ta itu med bestående brister i inmatningen av uppgifter i EU-databaserna och utbytet av information inom unionen.

Detta meddelande är ett första steg i ett förfarande mot interoperabilitet mellan informationssystemen, i syfte att strukturellt förbättra EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet. Kommissionen kommer att inrätta en expertgrupp för informationssystem och interoperabilitet för att bedöma de rättsliga, tekniska och operativa aspekterna av alternativen för att uppnå interoperabilitet mellan informationssystem och åtgärda eventuella brister och luckor. Efter det att expertgruppen lagt fram sina resultat kommer Europeiska kommissionen att presentera ytterligare konkreta idéer till Europaparlamentet och rådet vilket lägger grunden för en gemensam diskussion om hur man ska gå vidare. Kommissionen kommer också att höra datatillsynsmannen och de nationella dataskyddsmyndigheter som samlas i artikel 29-gruppen.

Målet bör vara utveckling av en gemensam strategi för att göra uppgiftshanteringen inom EU mer effektiv och ändamålsenlig, med fullt iakttagande av kraven på uppgiftsskydd, för att bättre skydda de yttre gränserna och förbättra den inre säkerheten, vilket gynnar alla medborgare.

## BILAGA 1: FÖRKORTNINGAR

|               |                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| Afis          | Automatiskt fingeravtrycksidentifieringssystem: ett system för tagning, lagring, jämförelse och kontroll av fingeravtryck |
| API-uppgifter | Förhandsinformation om passagerare                                                                                        |
| Ecris         | Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister                                           |
| EES           | Engelsk förkortning för det (föreslagna) in- och utresesystemet                                                           |
| EIS           | Europol's informationssystem                                                                                              |
| EIXM          | Den europeiska modellen för informationsutbyte                                                                            |
| Epris         | Ett europeiskt polisregisterindex                                                                                         |
| Etias         | (föreslaget) EU-system för reseuppgifter och resetillstånd                                                                |
| eu-LISA       | Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa            |
| Eurodac       | Europeiska daktyloskopisystemet (systemet för jämförelse av fingeravtryck)                                                |
| Europol       | Europeiska polisbyrån (Europeiska unionens brottsbekämpande byrå)                                                         |
| Find          | Interpols fasta nätverksdatabas                                                                                           |
| Frontex       | Europeiska byrån för förvaltningen av det operativa samarbetet vid Europeiska unionens medlemsstaters yttre gränser       |
| iARMS         | Interpols register- och spårningssystem för olagliga vapen                                                                |
| Interpol      | Internationella kriminalpolisorganisationen                                                                               |
| Mind          | Interpols mobila nätverksdatabas                                                                                          |
| PNR-uppgifter | Passageraruppgifter                                                                                                       |
| Prüm          | Polisiär samarbetsmekanism för utbyte av uppgifter om DNA, fingeravtryck och fordonsregistrering                          |
| SafeSeaNet    | En europeisk plattform för datautbyte för sjöfarten mellan medlemsstaternas sjöfartsmyndigheter                           |
| Siena         | Nätapplikation för säkert informationsutbyte                                                                              |
| SIS           | Schengens informationssystem (ibland kallat andra generationen av Schengens informationssystem – SIS II)                  |
| SLTD          | Engelsk förkortning för Interpols databas över stulna och förkomna resehandlingar                                         |
| s-Testa       | Säkra transeuropeiska telematiktjänster för myndigheter (kommer att uppgraderas till nästa generation, Testa-NG)          |
| TIS           | Tullinformationssystem                                                                                                    |
| UMF           | Universellt meddelandeformat för att möjliggöra kompatibilitet mellan informationssystem                                  |
| VIS           | Informationssystemet för viseringar                                                                                       |

## **BILAGA 2: FÖRTECKNING ÖVER BEFINTLIGA INFORMATIONSSYSTEM FÖR GRÄNSFÖRVALTNING OCH BROTTSBEKÄMPNING**

### **1. Schengens informationssystem (SIS)**

SIS är den största och mest använda plattformen för utbyte av uppgifter om immigration och brottsbekämpning. Det är ett centraliserat system som används av 25 EU-medlemsstater<sup>29</sup> och fyra Schengenassocierade länder<sup>30</sup>, och det innehåller för närvarande 63 miljoner registreringar. Dessa införs och konsulteras av behöriga myndigheter, såsom polis, gränskontroll och immigration. Systemet innehåller uppgifter om tredjelandsmedborgare som har nekats inresa eller vistelse inom Schengenområdet samt om EU-medborgare och tredjelandsmedborgare som är efterlysta eller försvunna (inklusive barn) och om efterlysta föremål (vapen, fordon, identitetshandlingar, industriutrustning osv.). Den egenskap som skiljer SIS från andra system för informationsutbyte är att uppgifterna kompletteras med instruktioner om konkreta åtgärder som ska vidtas av tjänstemän på fältet, såsom häktning eller beslagtagande.

Kontroller i SIS är obligatoriska för handläggning av viseringar för kortare vistelser, för gränskontroller av tredjelandsmedborgare och, på icke-systematisk basis<sup>31</sup>, för EU-medborgare och andra personer som åtnjuter rätt till fri rörlighet. Dessutom bör varje poliskontroll inom territoriet omfatta en automatisk kontroll i SIS.

### **2. Informationssystemet för viseringar (VIS)**

VIS är ett centraliserat system för utbyte av uppgifter mellan medlemsstaterna om viseringar för kortare vistelser. I systemet ingår uppgifter och beslut gällande ansökningar om viseringar för kortare vistelser för att besöka eller passera genom Schengenområdet. Alla Schengenstaternas konsulat (runt 2 000) och alla deras externa gränsövergångsställen (totalt ca 1 800) är uppkopplade till systemet.

VIS innehåller uppgifter om viseringsansökningar och beslut, samt huruvida utfärdade viseringar har återkallats, upphävts eller förlängts. För närvarande innehåller systemet uppgifter om 20 miljoner viseringsansökningar och vid rusningstider hanteras över 50 000 transaktioner i timmen. Varje viseringssökande uppger detaljerad biografisk information, ett digitalt fotografi och tio fingeravtryck. I sin nuvarande form är systemet ett tillförlitligt medel för att kontrollera viseringssökandes identitet, bedöma potentiella fall av irreguljär migration och säkerhetsrisker samt förhindra viseringsshopping.

Vid gränsövergångsställen eller inom medlemsstaternas territorium används VIS för att kontrollera viseringsinnehavares identitet genom att jämföra deras fingeravtryck med fingeravtrycken i VIS. Detta förfarande garanterar att den person som ansökte om viseringen är samma person som korsar gränsen. En sökning på fingeravtryck i VIS gör det också möjligt att identifiera en person som ansökt om visering under de fem senaste åren och som kanske saknar identitetshandlingar.

### **3. Eurodac**

Eurodac innehåller fingeravtryck för asylsökande och tredjelandsmedborgare som korsar Schengens yttre gränser på ett irreguljärt sätt. Systemets främsta syfte är för närvarande att avgöra vilket EU-land som är ansvarigt för att behandla en asylansökan, i enlighet

<sup>29</sup> Alla utom Irland, Cypern och Kroatien.

<sup>30</sup> Schweiz, Liechtenstein, Norge och Island.

<sup>31</sup> Denna regel kan ändras enligt kommissionens förslag COM(2015) 0670 om ändring av kodexen om Schengengränserna.

med Dublinförordningen. Systemet finns tillgängligt vid gränsövergångsställen, men i motsats till SIS och VIS är det inte ett gränsförvaltningssystem.

Fingeravtryck tas av irreguljära migranter som reser in i EU på ett olagligt sätt vid gränsövergångsställena. Dessa lagras i Eurodac för att bekräfta personens identitet i händelse av en framtida asylansökan. Immigrations- och polismyndigheterna kan också jämföra fingeravtrycksuppgifter från irreguljära migranter som påträffats i EU-medlemsstaterna för att kontrollera om personerna har ansökt om asyl i en annan medlemsstat. Brottsbekämpande myndigheter och Europol har också rätt att söka i Eurodac för att förhindra, upptäcka eller utreda ett grovt brott eller ett terroristbrott.

Registrering av asylsökandes eller irreguljära migranternas fingeravtryck i ett centraliserat system möjliggör identifiering och övervakning av deras sekundära rörelser<sup>32</sup> inom EU, tills en ansökan om internationellt skydd har lämnats in eller ett återsändandebeslut har fattats (i framtiden görs motsvarande registrering även i SIS). På ett mer allmänt plan krävs identifiering och övervakning av irreguljära migranter för att säkra att myndigheterna i deras ursprungsland utfärdar nya handlingar, och på så sätt underlätta deras återvändande.

#### **4. Interpols databas över stulna och förkomna resehandlingar**

Interpols databas över stulna och förkomna resehandlingar är en central databas för pass och andra resehandlingar som de utfärdande myndigheterna har anmält som stulna eller förkomna till Interpol. Detta innebär information om stulna blanka pass. Resehandlingar som anmälts som stulna eller förkomna till myndigheterna i länder som deltar i SIS registreras både i Interpols databas över stulna och förkomna resehandlingar och i SIS. Interpols databas över stulna och förkomna resehandlingar innehåller också uppgifter om resehandlingar som införts av länder som inte deltar i SIS (Irland, Kroatien, Cypern och tredjeländer).

Såsom fastslås i rådets slutsatser av den 9 och 20 november 2015 och i kommissionens förslag av den 15 december 2015 till en förordning om en riktad ändring av kodexen om Schengengränserna<sup>33</sup> bör resehandlingar som tillhör tredjelandsmedborgare och personer som åtnjuter fri rörlighet kontrolleras mot Interpols databas över stulna och förkomna resehandlingar. Alla gränsövergångsställen måste kopplas upp mot Interpols databas över stulna och förkomna resehandlingar. Dessutom skulle sökningar i Interpols databas över stulna och förkomna resehandlingar vid nationell brottsbekämpning ge ytterligare säkerhetsfördelar.

#### **5. Förhandsinformation om passagerare (API-uppgifter)**

Målet med API-uppgifterna är att insamla information om en persons identitet innan denna stiger ombord på ett flyg till EU och att identifiera irreguljära migranter vid ankomsten. API-uppgifterna består av information som ingår i en resehandling, såsom en resandes fullständiga namn, födelsedatum, nationalitet, resedokumentets nummer och typ, information om gränsövergångsstället för utresa och inresa samt transportuppgifter. API-uppgifter insamlas vanligen vid incheckningen.

Information före ankomst per sjötransport måste i enlighet med konventionen om förenkling av formaliteterna i internationell sjöfart inlämnas 24 timmar före fartygets

<sup>32</sup> Till exempel flyktingar som reser in i Grekland utan någon avsikt att ansöka om asyl i Grekland, utan reser till en annan medlemsstat landledes.

<sup>33</sup> Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EG) nr 562/2006 vad gäller stärkandet av kontrollerna mot relevanta databaser vid de yttre gränserna, COM(2015) 670 final.



beräknade ankomst. I direktiv 2010/65/EU<sup>34</sup> föreskrivs elektronisk dataöverföring via en enda kontaktpunkt som knyter samman SafeSeaNet, e-tull och andra elektroniska system.

Det finns inget centralt EU-system för registrering av API-uppgifter.

## **6. Europols informationssystem**

Europols informationssystem (EIS) är en centraliserad databas för kriminalunderrättelser i utredningssyfte. Det kan användas av medlemsstaterna och Europol för att lagra och söka uppgifter om grov brottslighet och terrorism. I EIS lagras uppgifter om personer, identitetshandlingar, bilar, vapen, telefonnummer, e-post, fingeravtryck, DNA och it-brottslighet. Uppgifterna kan sammankopplas på olika sätt för att skapa en mer detaljerad och strukturerad bild av ett brottsfall. EIS används för brottsbekämpningssamarbete och är inte tillgängligt för gränskontrollmyndigheter.

Informationsutbytet sker via plattformen Siena<sup>35</sup>, som är ett säkert elektroniskt kommunikationsnätverk mellan Europol, Europols sambandskontor, Europols nationella enheter, utsedda behöriga myndigheter (såsom tullen, kontor för återvinning av tillgångar osv.) och uppkopplade tredje parter.

I maj 2017 kommer en ny rättslig ram att börja tillämpas för Europol. Denna ram kommer att ge Europol utökade operativa möjligheter att göra analyser och lättare identifiera länkar mellan tillgänglig information.

## **7. Prümramen**

Prümramen baserar sig på ett multilateralt avtal<sup>36</sup> mellan medlemsstaterna som möjliggör utbyte av DNA, fingeravtryck och uppgifter ur fordonsregister. Konceptet baserar sig på sammankoppling av ett nationellt system med de nationella systemen i alla andra EU-medlemsstater, i syfte att möjliggöra korssökningar på distans. Då en sökning ger en träff i en annan medlemsstats databas delas detaljerade uppgifter om träffen genom bilaterala utbytesmekanismer.

## **8. Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris)**

Ecris är ett elektroniskt system för utbyte av uppgifter om tidigare fällande domar som brottmålsdomstolar i EU avkunnat mot en viss person, i syfte att användas vid brottmålsförfaranden mot en person och, om det tillåts enligt nationell lag, i andra syften. Vid fällande domar mot en medborgare i ett annat EU-land måste den medlemsstat där domen avkunnats meddela den medlemsstat där personen är medborgare om detta. Den medlemsstat där personen är medborgare måste lagra denna information och kan därför tillhandahålla uppdaterade kriminalregisteruppgifter om sina medborgare om sådana efterfrågas, oavsett var i EU den fällande domen avkunnades.

Ecris möjliggör också informationsutbyte om fällande domar mot tredjelandsmedborgare och statslösa personer. Särskilt utsedda centrala myndigheter i varje medlemsstat

---

<sup>34</sup> Europaparlamentets och rådets direktiv 2010/65/EU av den 20 oktober 2010 om rapporteringsformaliteter för fartyg som ankommer till och/eller avgår från hamnar i medlemsstaterna och om upphävande av direktiv 2002/6/EG.

<sup>35</sup> Nätapplikation för säkert informationsutbyte.

<sup>36</sup> Prümfördraget av 2005. Fördraget införlivades i EU-lagstiftningen 2008 genom rådets beslut 2008/615/RIF.

fungerar som kontaktpunkter i Ecris-nätverket, och hanterar alla uppgifter som att meddela, lagra, begära och tillhandahålla uppgifter ur kriminalregister.