EUROPA-
KOMMISSIONEN

Bruxelles, den 6.4.2016
COM(2016) 205 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Stærkere og mere intelligente informationssystemer for grænser og sikkerhed

1. INDLEDNING

Europa er et mobilt samfund. Millioner af EU-borgere og tredjelandsstatsborgere krydser hver dag de indre og ydre grænser. I 2015 var der mere end 50 millioner statsborgere fra lande uden for EU, som besøgte EU, og det betød mere end 200 millioner grænsepassager ved de ydre grænser til Schengenområdet.

Ud over de regulære rejsestrømme udløste konflikten i Syrien og kriser andre steder alene i 2015 1,8 millioner irregulære grænsepassager ved Europas ydre grænser. EU-borgerne forventer, at der er en effektiv kontrol af personer ved de ydre grænser, og at der er en effektiv forvaltning af migrationen, som bidrager til den indre sikkerhed. Terrorangrebene i Paris i 2015 og i Bruxelles i marts 2016 viste med al tydelighed, at der eksisterer en trussel mod den indre sikkerhed i Europa.

Dette betød, at der blev sat skarpere fokus på behovet for at gå sammen og gennemgribende styrke rammerne for EU's grænseforvaltning, migrations- og sikkerhedssamarbejde og informationsværktøjer. Grænseforvaltning, retshåndhævelse og migrationskontrol er dynamisk forbundne med hinanden. Vi ved, at der er EU-borgere, som har krydset de ydre grænser for at rejse til konfliktområder i terroristøjemed, og som udgør en risiko, når de vender tilbage. Der er flere beviser på, at terrorister har benyttet irregulære migrationsruter for at komme ind i EU og derefter frit er rejst rundt inden for Schengenområdet.

Den europæiske dagsorden om sikkerhed og den europæiske dagsorden om migration har angivet retningen for, hvordan EU's politik skal udvikles og gennemføres for at kunne håndtere de parallelle udfordringer ned forvaltning af migration og kampen mod terrorisme og organiseret kriminalitet. Denne meddelelse bygger på synergierne mellem disse to dagsordener og skal være et udgangspunkt for drøftelser om, hvordan eksisterende og kommende informationssystemer vil kunne forbedre både forvaltningen af de ydre grænser og den indre sikkerhed i EU. Den supplerer forslaget fra december 2015 om oprettelsen af en europæisk grænse- og kystvagt og om forbedring af kriseforebyggelse og intervention ved de ydre grænser.

På EU-plan er der flere informationssystemer, som kan give grænsevagter og politifolk relevante oplysninger om personer, men EU's dataforvaltningsstruktur er ikke perfekt. I denne meddelelse er der anført nogle forslag til, hvordan de eksisterende informationssystemer kan udnyttes bedre, og hvis det er nødvendigt, hvordan der kan udvikles nye og supplerende tiltag til at udfylde hullerne med. Det bliver også fremhævet, at det er nødvendigt at forbedre informationssystemernes interoperabilitet på lang sigt, sådan som også Det Europæiske Råd og Rådet har peget på[1]. Og der er anført ideer til, hvordan informationssystemer kan udvikles fremover for at sikre, at grænsevagter, toldmyndigheder, politifolk og retlige myndigheder kan få adgang til de oplysninger, som de har brug for.

Alle kommende initiativer vil blive baseret på principperne om bedre regulering med offentlige høringer og konsekvensanalyser, blandt andet hvad angår grundlæggende rettigheder og især retten til beskyttelse af personoplysninger.

[1] Konklusionerne fra Det Europæiske Råds møde den 17. og 18. december 2015. Fælles erklæring fra EU's justits- og indenrigsministre og EU-institutionernes repræsentanter om terrorangrebene den 22. marts 2016 i Bruxelles (24. marts 2016). Konklusioner vedtaget af EU-Rådet og medlemsstaterne, forsamlet i Rådet, om terrorbekæmpelse (20. november 2015).

2. UDFORDRINGER

Da der ikke er indre grænser i Schengenområdet, er det nødvendigt med en stærk og pålidelig styring af personers bevægelser over de ydre grænser. Det er en absolut forudsætning for at kunne have et højt internt sikkerhedsniveau og fri bevægelighed for personer inden for dette område. Og det betyder samtidig, at de retshåndhævende myndigheder i medlemsstaterne også har adgang til relevante oplysninger om personer. Der er en række informationssystemer og databaser på EU-plan, som kan give grænsevagter, politifolk og andre myndigheder oplysninger om personer, ud fra hvad der er relevant for deres respektive formål[2].

Der er dog også problemer med informationssystemerne, som vanskeliggør arbejdet for disse nationale myndigheder. Der blev derfor peget på bedre informationsudveksling som en af nøgleprioriteterne i den europæiske dagsorden om sikkerhed. Hovedproblemerne er: a) suboptimale funktioner i eksisterende informationssystemer, b) huller i EU's dataforvaltningsstruktur, c) et komplekst landskab med forskelligt styrede informationssystemer, og d) en fragmenteret struktur til dataforvaltning for grænsekontrol og sikkerhed.

De eksisterende informationssystemer i EU til grænseforvaltning og indre sikkerhed dækker en bred vifte af funktioner. Der er dog stadigvæk **problemer med funktionerne i de eksisterende systemer**. Hvis vi ser på grænsekontrolprocedurerne for forskellige kategorier af rejsende, bliver det klart, at der er problemer med nogle af disse procedurer og mellem de respektive informationssystemer, som benyttes til grænsekontrol. Også de eksisterende værktøjer til retshåndhævelse må kunne udnyttes bedre. Derfor må det overvejes, hvordan de eksisterende informationssystemer kan forbedres (afsnit 5).

Endvidere er der **huller i EU's dataforvaltningsstruktur**. Der er stadigvæk problemer med grænsekontrollen af specifikke kategorier af rejsende, såsom statsborgere fra tredjelande, som har et langtidsvisum. Der er også et problem med information forud for ankomst til grænsen for tredjelandsstatsborgere, som er fritaget for visumkravet. Det bør overvejes, om det er nødvendigt i givet fald at afhjælpe disse problemer ved at udvikle andre informationssystemer (afsnit 6).

For grænsevagter og især politifolk er der et **komplekst landskab med forskelligt styrede informationssystemer** på EU-plan. Det giver praktiske vanskeligheder især med hensyn til at se, hvilke databaser der skal benyttes i en given situation. Endvidere er det ikke alle medlemsstater, der er tilkoblet alle eksisterende systemer[3]. De nuværende vanskeligheder med at få adgang til informationssystemer på EU-plan vil kunne mindskes, hvis der indføres en fælles søgegrænseflade på nationalt plan, hvor der tages hensyn til de forskellige formål med adgangen (afsnit 7.1).

Den nuværende EU-struktur til dataforvaltning for grænsekontrol og sikkerhed er præget af **fragmentering**. Det skyldes de mange forskellige institutionelle, retlige og politiske sammenhænge, som systemerne er blevet udviklet i. Oplysninger bliver lagret separat i forskellige systemer, som kun sjældent er sammenkoblet med hinanden. Databaserne er ikke altid forenelige med hinanden, og de berørte myndigheder har ikke samme adgang til data. Det kan betyde blinde pletter for især de retshåndhævende myndigheder, da det kan være meget vanskeligt at se forbindelserne mellem datafragmenter. Det er derfor

[2] Se afsnit 4, hvor der er en oversigt over informationssystemer for grænser og sikkerhed, og bilag 2, hvor der er en mere detaljeret opgørelse.

[3] Under hensyn til de særlige betingelser i protokol 22 for så vidt angår Danmark og protokol 21 og 36 for så vidt angår Det Forenede Kongerige og Irland samt de respektive tiltrædelsesakter.

nødvendigt og hastende, at der arbejdes hen imod integrerede løsninger, som kan give bedre adgang til data for grænseforvaltning og sikkerhed under fuld hensyntagen til grundlæggende rettigheder. Til det formål må der sættes en proces i gang, som kan gøre de eksisterende informationssystemer interoperable (afsnit 7).

3. GRUNDLÆGGENDE RETTIGHEDER

En af de væsentlige forudsætninger for at tage fat om de ovennævnte udfordringer er fuld respekt for de grundlæggende rettigheder og databeskyttelsesreglerne.

For at kunne efterleve de grundlæggende rettigheder er det nødvendigt, at teknologi og informationssystemer er veludformede og anvendes korrekt. Teknologi og informationssystemer kan hjælpe offentlige myndigheder med at beskytte borgernes grundlæggende rettigheder. Med biometrisk teknologi kan risikoen for forveksling af identiteter og for diskrimination og racemæssig profilering mindskes. Det kan også være med til at beskytte børn mod risici, for eksempel børn, der forsvinder eller bliver ofre for menneskehandel, under forudsætning af at det sker under overholdelse af grundlæggende rettigheder og beskyttelsesforanstaltninger. Det kan mindske risikoen for, at folk bliver uberettiget anholdt og fængslet. Det kan også være med til at øge sikkerheden for borgere, der bor i Schengenområdet, da det vil bidrage til kampen mod terrorisme og grov kriminalitet.

Store informationssystemer kan også have konsekvenser for privatlivet, og det er nødvendigt at foregribe og afhjælpe risici i den forbindelse på passende måde. Indsamlingen og anvendelsen af personoplysninger i disse systemer har en indvirkning på retten til privatliv og på beskyttelsen af personoplysninger, som er forankret i Den Europæiske Unions charter om grundlæggende rettigheder. Alle systemer skal opfylde databeskyttelsesprincipperne og kravene til nødvendighed, proportionalitet, formålsbegrænsning og datakvalitet. Der skal være indført beskyttelsesforanstaltninger, som kan sikre registreredes rettigheder hvad angår beskyttelse af deres privatliv og personoplysninger. Data bør kun opbevares, så længe det er nødvendigt for det formål, som de er indsamlet til. Der skal kunne indsættes mekanismer, som kan sikre en præcis risikostyring og en effektiv beskyttelse af registreredes rettigheder.

I december 2015 nåede medlovgiverne til politisk enighed om databeskyttelsesreformen. Når den nye generelle forordning om databeskyttelse og direktivet om databeskyttelse for politimyndigheder og strafferetlige myndigheder bliver vedtaget og kommer til at gælde i 2018[4], vil vi have en harmoniseret ramme for behandling af personoplysninger.

Formålsbegrænsning er et af nøgleprincipperne i databeskyttelse og er forankret i chartret om grundlæggende rettigheder. På grund af de forskellige institutionelle, retlige og politiske sammenhænge, som informationssystemerne på EU-plan er blevet udviklet i, er princippet om formålsbegrænsning blevet gennemført ved en opdelt struktur til informationsforvaltning[5]. Det er en af årsagerne til den nuværende fragmentering i EU's struktur til dataforvaltning for grænsekontrol og indre sikkerhed. Når den nye omfattende ramme for beskyttelse af personoplysninger i EU er på plads, og der er sket en signifikant udvikling med hensyn til teknologi og IT-sikkerhed, vil princippet om formålsbegrænsning lettere kunne gennemføres, hvad angår adgang til og anvendelse af lagrede data i fuld overensstemmelse med chartret om grundlæggende rettigheder og med seneste retspraksis hos EU-Domstolen. Med beskyttelsesforanstaltninger såsom opdeling

[4] Se http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[5] KOM(2010) 385 endelig.

af data inden for ét system og specifikke regler for adgang og anvendelse for hver data- og brugerkategori vil der kunne sikres den fornødne formålsbegrænsning i integrerede løsninger til dataforvaltning. Det åbner vejen for interoperabilitet mellem informationssystemer med de fornødne strikte regler for adgang og anvendelse, uden at det påvirker den eksisterende formålsbegrænsning.

"Indbygget databeskyttelse" og "databeskyttelse gennem indstillinger" er nu nogle af principperne i EU's regler om databeskyttelse. Kommissionen vil forsøge at følge dette princip, når der udvikles nye instrumenter, som skal baseres på anvendelse af informationsteknologi. Det betyder, at beskyttelse af personoplysninger skal indarbejdes i det teknologiske grundlag for et givet instrument, at databehandling skal begrænses til, hvad der er nødvendigt for et bestemt formål, og at der kun gives adgang til oplysningerne til de enheder, der har "behov for at få kendskab" til oplysninger"[6].

Kravene i chartret om grundlæggende rettigheder og især de nye reforminstrumenter til databeskyttelse vil være en hjælp for Kommissionen til at afhjælpe de nuværende huller og mangler i EU's struktur til dataforvaltning for grænsekontrol og sikkerhed. Det vil sikre, at yderligere udvikling af informationssystemer på disse områder vil være på linje med de højeste standarder for databeskyttelse, og at de vil opfylde og bidrage til grundlæggende rettigheder, sådan som det er garanteret i chartret om grundlæggende rettigheder.

4. OVERSIGT OVER INFORMATIONSSYSTEMER FOR GRÆNSER OG SIKKERHED[7]

De eksisterende informationssystemer i EU til grænseforvaltning og indre sikkerhed har hver især deres mål, formål retsgrundlag[8], brugergrupper og institutionel kontekst. De udgør tilsammen et komplekst mønster af relevante databaser.

De tre vigtigste **centraliserede informationssystemer**, som er udviklet af EU, er i) Schengeninformationssystemet (SIS) med et bredt spektrum af indberetninger om personer og genstande, ii) visuminformationssystemet (VIS) med data om visa til kortvarigt ophold og iii) EURODAC-systemet med fingeraftryksdata om asylansøgere og tredjelandsstatsborgere, som på iregulær vis har krydset de ydre grænser. Disse tre systemer supplerer hinanden og er – med undtagelse af SIS – primært rettet mod statsborgere fra tredjelande. Systemerne er også en hjælp for nationale myndigheder i deres kamp mod kriminalitet og terrorisme[9]. Dette gælder især SIS, som er det informationsdelingsinstrument, der er mest anvendt i dag. Informationsudvekslingen mellem disse systemer foregår inden for en sikret særlig kommunikationsinfrastruktur, som kaldes sTESTA[10].

---

6 For at få en samlet beskrivelse af "privacy by design" henvises der til udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om styrkelse af tilliden til informationssamfundet ved at styrke databeskyttelsen og privatlivets fred, Den Europæiske Tilsynsførende for Databeskyttelse, 18.3.2010.

7 Der henvises til bilag 2 for en opgørelse over eksisterende informationssystemer til grænseforvaltning og retshåndhævelse.

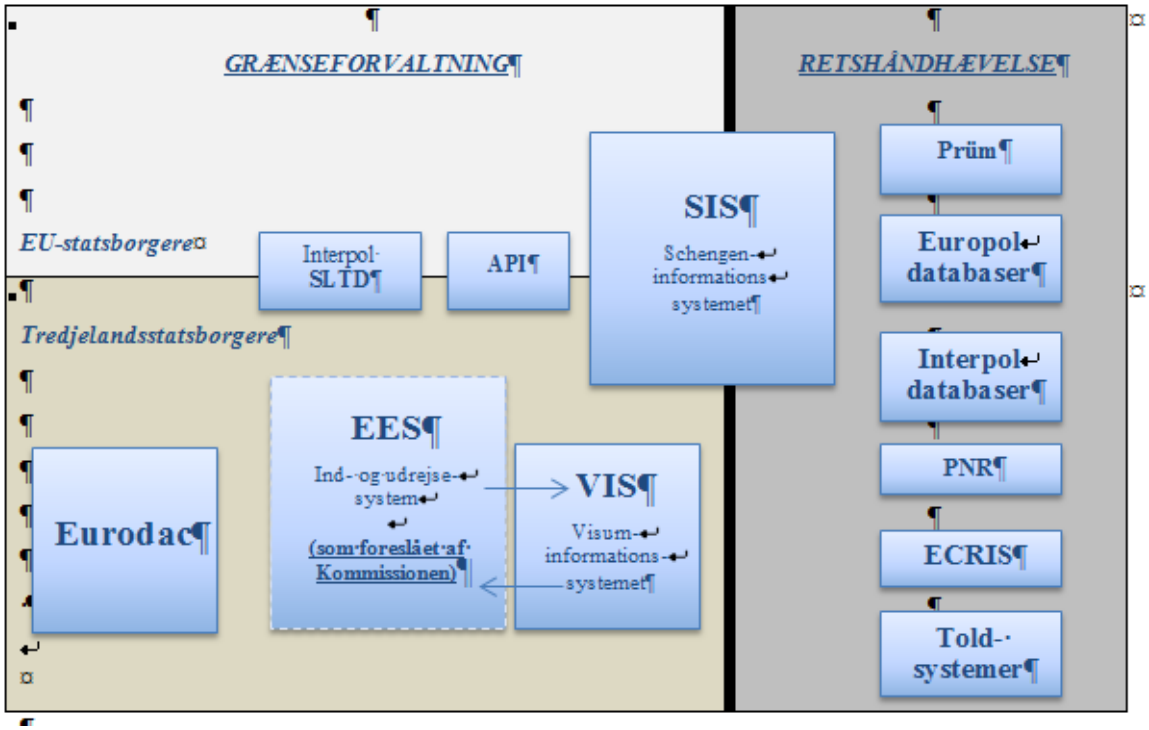
8 Under hensyn til de særlige betingelser i protokol 22 for så vidt angår Danmark og protokol 21 og 36 for så vidt angår Det Forenede Kongerige og Irland.

9 I retshåndhævelsesøjemed kan der gives adgang til VIS og EURODAC under begrænsede betingelser, idet retshåndhævelse er et underordnet formål i disse systemer. For VIS' vedkommende skal medlemsstaterne udpege en myndighed, der skal have ansvaret for at kontrollere adgang i retshåndhævelsesøjemed, og politiet skal fremlægge bevis for, at deres adgang er nødvendig for efterforskning i en kriminalsag. For EURODAC's vedkommende skal efterforskningsmyndigheden først søge i de nationale systemer, AFIS, Prüm og VIS, inden de kan få adgang til EURODAC.

10 Vil snart blive erstattet af TESTA-NG.

Ud over disse eksisterende systemer foreslår Kommissionen, at der bliver oprettet et fjerde centraliseret grænseforvaltningssystem, **ind- og udrejsesystemet** (EES)[11], som forventes gennemført inden 2020, og som også er rettet mod statsborgere fra tredjelande.

Figur 1 *Skematisk oversigt over de vigtigste informationssystemer til grænseforvaltning og retshåndhævelse:*



Af andre eksisterende instrumenter til grænseforvaltning er der Interpols databaser over henholdsvis stjålne og bortkomne rejsedokumenter (SLTD) og forhåndsinformation om passagerer (API), hvor der indsamles information om passagerer forud for flyvninger til EU. Disse instrumenter vedrører både EU-borgere og tredjelandsstatsborgere.

EU har specifikt med henblik på retshåndhævelse, kriminalefterforskning og retligt samarbejde udviklet **decentraliserede værktøjer til informationsudveksling**, nemlig i) Prümrammen til at udveksle DNA, fingeraftryk og registreringsdata for køretøjer og ii) det europæiske informationssystem vedrørende strafferegistre (ECRIS) til at udveksle nationale oplysninger fra strafferegistre. Ved hjælp af ECRIS kan der udveksles oplysninger gennem sikrede netværk om tidligere domme, som er afsagt mod en bestemt person af straffedomstole i Den Europæiske Union. Anmodningerne drejer sig primært om alfanumeriske identitetsoplysninger, men det er også muligt at udveksle biometriske data.

Europol fungerer som EU's knudepunkt for oplysninger om kriminalitet og støtter udvekslingen af oplysninger mellem nationale politimyndigheder. Europols informationssystem (EIS) er en centraliseret database med strafferetlige oplysninger, hvor medlemsstaterne kan lagre og forespørge data over grov kriminalitet og terrorisme. Der er kontaktpunkter i Europol, som arbejder med emnerettede analyser og giver oplysninger om igangværende operationer i medlemsstaterne. Med Europols netværksapplikation til sikker informationsudveksling (SIENA) kan medlemsstaterne udveksle oplysninger på en hurtig, sikker og brugervenlig måde med hinanden, med Europol eller med tredjeparter, der har en samarbejdsaftale med Europol. Samtidig er der

[11] COM(2016)194 final.

i SIENA stærk fokus på interoperabilitet med andre systemer i Europol, for eksempel for direkte at kunne udveksle data med kontaktpunkter. Det giver mulighed for at kunne indføre oplysninger i Europols databaser, som medlemsstaterne har udvekslet med hinanden. SIENA bør derfor være medlemsstaternes første valg, når det drejer sig om at udveksle oplysninger om retshåndhævelse inden for EU.

Der er et andet sæt af systemer til behandling af personoplysninger, som vil blive udviklet i medlemsstaterne, nemlig **passagerlister** (PNR)[12]. PNR-data er booking-oplysninger, som gives på tidspunktet for booking og check-in.

Endelig er også **toldmyndighederne** afgørende aktører i samarbejdet ved de ydre grænser mellem de forskellige agenturer. De har forskellige systemer[13] og databaser, som indeholder data over varebevægelser, identifikation af økonomiske operatører og risikorelaterede oplysninger, der kan anvendes til at styrke den indre sikkerhed. Disse systemer har også deres egen kontrollerede, restriktive og sikre infrastruktur (fælles kommunikationsnet), som har vist sig at kunne fungere. Der bør ses nærmere på, om der kan opnås synergier og konvergens mellem informationssystemer og deres tilsvarende infrastrukturer for EU's grænseforvaltning og for toldoperationer.

5. FORBEDRING AF EKSISTERENDE INFORMATIONSSYSTEMER

De eksisterende informationssystemer i EU til grænseforvaltning og indre sikkerhed dækker en bred vifte af funktioner. Men der er stadigvæk **mangler** i systemerne, som det er nødvendigt at afhjælpe, hvis de skal kunne fungere optimalt.

Schengeninformationssystemet (SIS)

Grænsekontrol baseret på **Schengeninformationssystemet** (SIS) sker for øjeblikket ud fra alfanumeriske søgninger (dvs. navn og fødselsdato). Fingeraftryk kan kun anvendes til at verificere og bekræfte identiteten på en person, som allerede er blevet identificeret ud fra sit navn. På grund af dette sikkerhedshul kan personer, der er omfattet af en indberetning, benytte falske dokumenter og dermed undgå en nøjagtig match i SIS.

Denne alvorlige svaghed vil blive afhjulpet ved, at der tilføjes en søgefunktion for fingeraftryk i SIS gennem et **automatisk fingeraftryksidentifikationssystem (AFIS)**, sådan som det er fastsat i den eksisterende lovramme[14]. AFIS vil kunne være operationelt fra midten af 2017[15]. Når AFIS er færdigudviklet, vil der være adgang hertil for Europol, og det vil hermed supplere Europols systemer til strafferetlig efterforskning og bekæmpelse af terrorisme samt udvekslinger af fingeraftryk, der foregår inden for Prümrammen. Kommissionen og eu-LISA vil se nærmere på, om det er muligt at anvende det kommende AFIS i et sådant bredere øjemed.

---

[12] Se afsnit 6.2.

[13] Toldinformationssystemerne omfatter alle systemer, der er oprettet i medfør af EF-toldkodeksen (forordning 2913/92) og den kommende EU-toldkodeks (forordning 952/2013), afgørelsen om papirløse rammer for told og handel (beslutning 70/2008/EF) samt toldinformationssystemet CIS, der blev oprettet i medfør af CIS-konventionen af 1995. Hensigten hermed er at bekæmpe toldrelateret kriminalitet ved at lette samarbejdet mellem europæiske toldmyndigheder.

[14] Artikel 22, litra c), i Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) og Rådets afgørelse 533/2007/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 381 af 28.12.2006, s. 4, og EUT L 205 af 7.8.2007, s. 63).

[15] I marts 2016 forelagde Kommissionen en rapport for Europa-Parlamentet og Rådet om tilgængeligheden og den umiddelbare anvendelighed af teknologi til identificering af personer på grundlag af fingeraftryk, der er lagret i anden generation af Schengeninformationssystemet (SIS II).

Ud fra den igangværende evaluering og en teknisk undersøgelse er Kommissionen for øjeblikket ved at se på **muligheden for andre funktioner i SIS** med henblik på at fremlægge forslag til revision af retsgrundlaget for SIS. Blandt de aspekter, der overvejes, er følgende:

- indførelse af SIS-indberetninger om irregulære migranter, der er genstand for afgørelser om tilbagesendelse
- anvendelse af ansigtsbilleder til biometrisk identifikation, ud over fingeraftryk
- automatiseret videregivelse af oplysninger om et hit efter en kontrol
- lagring af hitoplysninger om indberetninger om diskret og målrettet kontrol i SIS's centrale system
- oprettelse af en ny indberetningskategori om "Eftersøgt ukendt person", som der kan være kriminaltekniske data om i nationale databaser (f.eks. et latent aftryk på et gerningssted)[16].

Kommissionen vil fortsætte med at give EU-midler til gennemførelse af projekter, som gør det muligt at foretage simultane søgninger i SIS og Interpols databaser over stjålne og bortkomne rejsedokumenter (SLTD) og eftersøgte kriminelle personer, køretøjer og skydevåben (iArms), som supplerer EU's informationssystemer[17].

Interpols database over stjålne og bortkomne rejsedokumenter (SLTD)

Det er af afgørende betydning for en effektiv grænseforvaltning, at alle tredjelandsstatsborgeres og EU-borgeres rejsedokumenter bliver verificeret i forhold til **SLTD-databasen**. De retshåndhævende myndigheder bør også benytte SLTD-databasen til forespørgsler inden for Schengenområdet. Efter terrorangrebene i Paris den 13. november 2015 ønskede Rådet, at der inden udgangen af marts skulle være etableret elektronisk tilkobling til Interpols relevante databaser på alle overgangssteder ved de ydre grænser og automatisk screening af rejsedokumenter[18]. Alle medlemsstater skulle etablere de relevante elektroniske tilkoblinger og indføre systemer, hvormed det bliver muligt at opdatere data over stjålne og bortkomne rejsedokumenter i SLTD-databasen.

Forhåndsinformation om passagerer (API)

Medlemsstaterne bør ud fra eksisterende bedste praksis også øge merværdien af **forhåndsinformation om passagerer** (AIP-data) og etablere automatiske krydstjek af disse data i forhold til SIS og Interpols SLTD-database. Kommissionen vil se på, om det er nødvendigt at revidere retsgrundlaget for behandling af API-data for at sikre en bredere gennemførelse og for at indføre en forpligtelse for medlemsstaterne til at kræve og benytte API-data for alle indgående og udgående flyvninger. Det er især relevant i forbindelse med gennemførelsen af det kommende direktiv om passagerlister (PNR), eftersom det vil være langt mere effektivt at kombinere PNR-data med API-data for at bekæmpe terrorisme og grov kriminalitet[19].

---

[16] Indførelsen af denne nye indberetning vil blive taget op til vurdering for at se, om den kan supplere den eksisterende Prüm-ramme til søgning af fingeraftryk i de forskellige nationale databaser i EU-medlemsstaterne, og for at undgå overlapning i den forbindelse.

[17] Informationssøgeværktøjer, som er udviklet af Interpol, såsom Fixed Interpol Networked Database (FIND) og Mobile Interpol Networked Database (MIND), har til formål at gøre det lettere at foretage simultane søgninger i Interpols systemer og i SIS.

[18] Konklusioner vedtaget af EU-Rådet og medlemsstaterne, forsamlet i Rådet, om terrorbekæmpelse, 20. november 2015.

[19] Der henvises til afsnit 6.2 for det foreslåede direktiv om navnelister (PNR).

Visuminformationssystemet (VIS)

Kommissionen er også i gang med at foretage en overordnet evaluering af **visuminformationssystemet** (VIS), som det er meningen skal være afsluttet i 2016. Under evalueringen ses der blandt andet på, hvordan VIS bliver anvendt til kontrol ved de ydre grænser og inden for medlemsstaternes eget område, og hvordan det bidrager til kampen mod identitets- og visumsvindel. På grundlag heraf vil Kommissionen så undersøge muligheden af at forbedre funktionerne i VIS, blandt andet ved:

- at forbedre kvaliteten af ansigtsbilleder, så det bliver muligt at foretage biometrisk match
- at anvende biometriske data for visumansøgere til søgninger det kommende automatiske fingeraftryksidentifikationssystem, som skal udvikles til SIS
- at nedsætte aldersgrænsen for indsamling af fingertryk af børn i alderen fra 6 til 12 år, og samtidig sørge for solide foranstaltninger til beskyttelse af grundlæggende rettigheder og andre beskyttelsesforanstaltninger[20]
- at gøre det lettere at tjekke Interpols SLTD-database under en visumansøgning.

Med hensyn til mulighederne for under den eksisterende lovramme at få adgang til VIS-data i **retshåndhævelsesøjemed** så anvender medlemsstaterne disse muligheder på forskellig måde. I den forbindelse har medlemsstaterne meldt om praktiske problemer, som retshåndhævende myndigheder har haft med at få adgang til VIS. Gennemførelsen af adgang til EURODAC i retshåndhævelsesøjemed er ligeledes stadigvæk meget begrænset. Kommissionen vil se på, om der er behov for at gøre noget ved den retlige ramme for adgang til VIS og EURODAC i retshåndhævelsesøjemed.

EURODAC

Som det fremgår af meddelelsen om en reform af det fælles europæiske asylsystem og fremme af lovlige migrationsveje til Europa[21], vil Kommissionen fremlægge et forslag til reform af **EURODAC** for at forbedre dets funktioner vedrørende irregulær migration og tilbagesendelse. Det vil afhjælpe det nuværende problem vedrørende muligheden for at opspore irregulære migranters sekundære bevægelser mellem medlemsstater. Endvidere vil det med forslaget blive forsøgt at gøre tilbagesendelses- og tilbagetagelsesprocedurer mere effektive ved at sørge for, at der er midler til at identificere irregulære migranter og udstede nye papirer til dem med henblik på tilbagesendelse. I den forbindelse vil forslaget også dække udveksling med tredjelande af oplysninger i EURODAC under iagttagelse af de databeskyttelsesforanstaltninger, der er nødvendige.

Europol

EU har givet **Europol** adgang til de vigtigste centrale databaser, men agenturet har endnu ikke fuldt ud benyttet sig af denne mulighed. Europol har ret til adgang og til direkte at søge i data, der er registreret i SIS om anholdelser, om diskret og målrettet kontrol og om genstande, der skal beslaglægges. Europol har hidtil kun foretaget et relativt begrænset antal søgninger i SIS. Det har siden september 2013 været retligt muligt for Europol at konsultere VIS. Siden 2015 har retsgrundlaget for EURODAC tilladt Europol at få adgang. Agenturet bør fremskynde det igangværende arbejde med at etablere tilkoblingen til VIS og EURODAC. Mere generelt vil Kommissionen se på, om det er nødvendigt at give yderligere adgang for andre EU-agenturer inden for indre anliggender til informationssystemer, navnlig for den kommende europæiske grænse- og kystvagt.

[20] Angivet som teknisk gennemførligt i JRC-undersøgelsen "Fingerprint Recognition for children" (om fingeraftryksgenkendelse for børn), EUR 26193 EN, ISBN 978-92-79-33390-3Children', 2013.

[21] COM(2016) 197 final.

Prümrammen

Prümrammen bliver for øjeblikket ikke udnyttet fuldt ud. Det skyldes, at ikke alle medlemsstater har opfyldt deres retmæssige forpligtelser hvad angår integrationen af netværket i deres egne systemer. Medlemsstaterne har fået betydelig finansiel og teknisk støtte til gennemførelsen heraf og bør nu gennemføre Prümrammen fuldt ud. Kommissionen benytter de beføjelser, den har fået overdraget til at sikre, at medlemsstaterne opfylder deres retmæssige forpligtelser fuldt ud, og indledte i januar 2016 en struktureret dialog (EU-Pilot) med berørte medlemsstater. Hvis svarene fra medlemsstaterne viser sig ikke at være tilfredsstillende, vil Kommissionen ikke tøve med at indlede traktatbrudssager.

Det europæiske informationssystem vedrørende strafferegistre (ECRIS)

Det europæiske informationssystem vedrørende strafferegistre **ECRIS** giver mulighed for at udveksle oplysninger om domme over tredjelandsstatsborgere og statsløse personer, men der er ingen procedure til at gøre dette på en effektiv måde. I januar 2016 vedtog Kommissionen et lovforslag, som skulle afhjælpe denne mangel[22]. I den forbindelse foreslog Kommissionen, at det skulle være muligt for nationale myndigheder at søge efter tredjelandsstatsborgere på grundlag af fingeraftryk for at opnå en mere sikker identifikation. Europa-Parlamentet og Rådet vil kunne vedtage lovgivningsteksten i 2016.

Horisontale spørgsmål

Et generelt problem med hensyn til informationssystemer er, **i hvor høj grad medlemsstaterne har gennemført dem**. Den uensartede gennemførelse af Prümrammen og de manglende elektroniske tilkoblinger til SLTD-databasen er slående eksempler herpå. For at gennemførelsen af informationssystemer kan blive bedre, vil Kommissionen holde nøje øje med, hvad der sker i hver enkelt medlemsstat[23]. Der vil ikke blot blive holdt øje med, om medlemsstaterne opfylder deres retmæssige forpligtelser hvad angår informationssystemer, men også med, hvordan de gør brug af eksisterende instrumenter, og om de følger bedste praksis. Kommissionen vil trække på forskellige kilder, når den overvåger og fremskynder gennemførelsen, blandt andet meddelelser fra medlemsstaterne og besøg, der gennemføres inden for rammerne af Schengenevaluerings- og overvågningsmekanismen.

Et andet generelt problem med hensyn til informationssystemer er **kvaliteten af de indførte data**. Hvis medlemsstaterne ikke respekterer minimumskravene til kvalitet, bliver pålideligheden og værdien af de lagrede data meget begrænset, og risikoen for fejlagtige match og manglende hits undergraver værdien af selve systemerne. For at forbedre kvaliteten af de data, der indføres, vil eu-LISA udvikle en **central overvågningskapacitet for datakvalitet** for alle systemer, som hører under dets kompetence.

De fleste informationssystemer inden for området grænsekontrol og sikkerhed forvalter identifikationsdata, der kommer fra rejse- og ID-dokumenter. For at forstærke grænserne og sikkerheden er det ud over at have velfungerende systemer nødvendigt let og sikkert at kunne få bekræftet ægtheden af rejse- og identitetsdokumenter. Med henblik herpå vil Kommissionen foreslå foranstaltninger, der kan forbedre elektronisk **dokumentsikkerhed** og ID-forvaltning og styrke kampen mod dokumentforfalskning.

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

[23] Under hensyn til de særlige betingelser i protokol 22 for så vidt angår Danmark og protokol 21 og 36 for så vidt angår Det Forenede Kongerige og Irland.

De interoperable niveauer for sikker identifikation, som kan opnås ved hjælp af eIDAS-forordningen[24], kan være en måde at gøre dette på.

Tiltag til at forbedre eksisterende informationssystemer

Schengeninformationssystemet (SIS)

- Kommissionen og eu-LISA udvikler og indfører en funktion med automatiseret fingeraftryksidentifikationssystem (AFIS) i SIS senest midt i 2017.
- Kommissionen forelægger inden udgangen af 2016 forslag om revision af retsgrundlaget for SIS for yderligere at forbedre dets funktion.
- Medlemsstaterne øger deres brug af SIS, både ved at indføre alle relevante oplysninger og ved at konsultere systemet, når som helst det er nødvendigt.

Interpols database over stjålne og bortkomne rejsedokumenter (SLTD)

- Medlemsstaterne opretter elektroniske tilkoblinger til Interpols værktøjer ved alle deres overgangssteder ved de ydre grænser.
- Medlemsstaterne opfylder deres forpligtelse til at indføre og konsultere data over stjålne eller bortkomne rejsedokumenter samtidigt i både SIS og SLTD-databasen.

Forhåndsinformation om passagerer (API)

- Medlemsstaterne automatiserer brugen af API-data ved kontrol i SIS og Interpols database over stjålne og bortkomne rejsedokumenter (SLTD) på linje med eksisterende bedste praksis.
- Kommissionen vurderer, om det er nødvendigt at revidere retsgrundlaget for behandlingen af API-data.

Visuminformationssystemet (VIS)

- Kommissionen ser på, hvordan VIS kan forbedres yderligere inden udgangen af 2016.

EURODAC

- Kommissionen fremlægger et forslag om revision af retsgrundlaget for EURODAC for yderligere at forbedre dets funktioner hvad angår irregulær migration og tilbagesendelse.

Europol

- Europol udnytter sin eksisterende ret fuldt ud til at konsultere SIS, VIS og EURODAC.
- Kommissionen og Europol udforsker og fremmer synergier mellem Europols informationssystem (EIS) og andre systemer, navnlig SIS.
- Kommissionen og eu-LISA ser på, om det automatiserede fingeraftryksidentifikationssystem (AFIS), der skal udvikles for SIS, kan supplere Europols systemer til strafferetlig efterforskning og bekæmpelse af terrorisme.

[24] Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Prümrammen

- Medlemsstaterne gennemfører og anvender Prümrammen i fuldt omfang.
- Hvis det er nødvendigt indleder Kommissionen traktatbrudssager mod medlemsstater, som ikke har tilkoblet sig Prümrammen.
- Kommissionen og eu-LISA ser på, om det automatiserede fingeraftryksidentifikationssystem (AFIS), der skal udvikles for SIS, kan supplere udveksling af fingeraftryksdata under Prümrammen.

Det europæiske informationssystem vedrørende strafferegistre (ECRIS)

- Europa-Parlamentet og Rådet vil i 2016 kunne vedtage lovgivningsforslaget om at give nationale myndigheder mulighed for at søge efter tredjelandsstatsborgere i ECRIS på grundlag af fingeraftryk.

Horisontale spørgsmål

- Kommissionen **overvåger og fremmer gennemførelsen** af informationssystemer.
- eu-LISA udvikler en **central overvågningskapacitet for datakvalitet** for alle systemer, som hører under dets kompetence.
- Kommissionen foreslår foranstaltninger, der kan forbedre elektronisk **dokumentsikkerhed og ID-forvaltning** og styrke kampen mod dokumentforfalskning.
- Kommissionen ser nærmere på, om der kan opnås synergier og konvergens mellem informationssystemer og deres tilsvarende infrastrukturer for EU's grænseforvaltning og for **toldoperationer**.

6. UDVIKLING AF EKSTRA INFORMATIONSSYSTEMER OG AFHJÆLPNING AF HULLER

De eksisterende informationssystemer dækker over et bredt spektrum af data, som er nødvendige for grænseforvaltning og retshåndhævelse, men der er også store huller. Nogle af disse huller er der taget fat om af Kommissionen i lovgivningsforslag, nemlig forslagene om et ind-og udrejsesystem og om en EU-ordning om passagerlister (PNR). For de andre huller, som er blevet konstateret, er det nødvendigt med en omhyggelig vurdering for at se, om der er behov for andre EU-værktøjer.

1. Ind- og udrejsesystem

Kommissionen har fremlagt de reviderede lovgivningsforslag om oprettelse af et ind- og udrejsesystem (EES) samtidig med denne meddelelse. Når systemet er blevet vedtaget af medlovgiverne, vil det være eu-LISA, der skal udvikle og gennemføre systemet sammen med Schengenmedlemsstaterne.

I EES vil der blive registreret grænsepassage (ind- og udrejse) for alle tredjelandsstatsborgere, der besøger Schengenområdet for kortvarigt ophold (maksimalt 90 dage inden for en periode på 180 dage), både rejsende, som skal have visum, og rejsende, som er fritaget for visumkravet, eller ophold på grundlag af det nye turistvisum (op til ét år). Målene for EES er a) at forbedre forvaltningen af de ydre grænser, b) at mindske irregulær migration og hindre, at folk opholder sig længere end tilladt, og c) at bidrage til kampen mod terrorisme og grov kriminalitet, for derved at bidrage til at sikre et højt niveau for indre sikkerhed.

I EES vil identiteten på tredjelandsstatsborgere blive registreret (alfanumeriske data, fire fingeraftryk og ansigtsbillede) sammen med oplysninger fra deres rejsedokumenter, og dette vil blive koblet til elektroniske oplysninger om ind- og udrejse. Den nuværende praksis med stempling af rejsedokumenter vil ophøre. Med EES vil det være muligt

effektivt at forvalte godkendte kortvarige ophold, at øge automatiseringen ved grænsekontrol og at forbedre opsporingen af dokument- og identitetsforfalskning. Med en central registrering vil det blive muligt at opspore folk, der opholder sig længere end tilladt, og identificere personer uden papirer i Schengenområdet. Det foreslåede EES udfylder derfor et stort hul i de eksisterende informationssystemer.

2. Passagerlister

Passagerlistedata (PNR-data) er bookingoplysninger med konkrete detaljer, fuldstændige rejse- og reservationsdetaljer, særlige bemærkninger, plads- og baggageoplysninger, betalingsmiddel. PNR-data er nyttige og nødvendige for at kunne identificere højrisikorejsende med henblik på bekæmpelse af terrorisme, narkotikahandel, menneskehandel, seksuelt misbrug af børn og anden grov kriminalitet. Det foreslåede PNR-direktiv vil sikre et bedre samarbejde mellem de nationale systemer og mindske sikkerhedshullerne mellem medlemsstaterne. Det foreslåede PNR-direktiv opfylder derfor et stort hul i de tilgængelige data, som er nødvendige for at kunne bekæmpe grov kriminalitet og terrorisme. **PNR-direktivet bør vedtages og gennemføres som et hasteanliggende**.

Ifølge det kommende direktiv vil medlemsstaterne skulle oprette passagerinformationsenheder (PIU), der vil få PNR-data fra luftfartsselskaber. Det betyder ikke, at der skal oprettes et centralt system eller en central database, men der vil blive en vis grad af standardisering af nationale tekniske løsninger og procedurer. Dermed bliver det lettere at udveksle PNR-data mellem disse enheder, som det fremgår af det foreslåede direktiv. Til det formål vil Kommissionen hjælpe medlemsstaterne med at analysere forskellige scenarier for sammenkobling mellem enheder for at finde standardiserede løsninger og procedurer. Når direktivet er blevet vedtaget, vil Kommissionen fremskynde arbejdet med fælles protokoller og understøttede dataformater til overførsel af PNR-data fra luftfartsselskaber til disse enheder. Kommissionen vil udarbejde et udkast til gennemførelsesakt inden for tre måneder efter vedtagelsen af direktivet.

3. Informationshul forud for ankomst af tredjelandsstatsborgere, der er fritaget for visumkravet

For visumindehavere registreres identitets-, kontakt- og baggrundsoplysninger i VIS, mens det for personer, der er fritaget for visumkravet, kun er oplysninger fra deres rejsedokumenter, der registreres. For rejsende, der ankommer med fly eller med skib, kan dette suppleres forud for ankomsten med API-data. Ifølge det foreslåede PNR-direktiv vil deres PNR-data også blive indsamlet, hvis de ankommer til EU med fly. For personer, der kommer ind i EU via landegrænser, er der ingen oplysninger til rådighed forud for deres ankomst til EU's ydre grænser.

De retshåndhævende myndigheder kan indhente oplysninger om visumindehavere fra VIS, hvis det er nødvendigt for at bekæmpe grov kriminalitet og terrorisme, men der er ingen tilsvarende data tilgængelige om personer, der er fritaget for visumkravet. Denne mangel på oplysninger er især relevant for forvaltningen af EU's landegrænser i en situation, hvor et stort antal rejsende, som er fritaget for visumkravet, ankommer med bil, bus eller tog. Mange af nabolandene til EU er allerede fritaget for visumkravet, og der er liberaliseringsdialoger i gang mellem EU andre af nabolandene. Det vil sandsynligvis i nær fremtid føre til en betydelig stigning i antallet af rejsende, som er fritaget for visumkravet.

Kommissionen vil se nærmere på, om det er nødvendigt, gennemførligt og proportionelt med et nyt EU-værktøj til at håndtere dette. En af de muligheder, der kan overvejes, er et

EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS), hvor rejsende, der er fritaget for visumkravet, skal registrere relevante oplysninger om deres påtænkte rejse. Den automatiske behandling af disse oplysninger vil være en hjælp for grænsevagterne, når de skal vurdere besøgende fra tredjelande, der ankommer for et kortvarigt ophold. Lande som USA, Canada og Australien har allerede indført sådanne systemer, også for EU-borgere.

Rejsetilladelsessystemer er baseret på onlineansøgninger, hvor ansøgeren giver oplysninger om identitet, kontaktoplysninger, formål med rejsen, rejserute osv. inden afrejsen. Når denne tilladelse foreligger, bliver grænseprocedurerne hurtigere og smidigere. Ud over de fordele, som det giver for sikkerhed og grænseforvaltning og potentiel gensidighed på visumområdet, vil et system som ETIAS derfor også kunne gøre det lettere for rejsende.

4. Europæisk informationssystem vedrørende politiregistre (EPRIS)

Som angivet i den europæiske dagsorden om sikkerhed er adgang til eksisterende oplysninger i realtid på tværs af medlemsstaterne et af de fremtidige indsatsområder, hvad angår informationsudveksling. Kommissionen vil se nærmere på, hvor nødvendigt, teknisk gennemførligt og proportionelt et europæisk politiregistereindekssystem (EPRIS) kan være til at lette grænseoverskridende adgang til oplysninger, der opbevares i nationale databaser over retshåndhævelse. I den forbindelse giver Kommissionen EU-midler til et pilotprojekt, som gennemføres af en gruppe på fem medlemsstater, og som vedrører oprettelse af en mekanisme til automatiserede grænseoverskridende søgninger i nationale indekser på grundlag af "hit/intet hit"[25]. Kommissionen vil tage resultaterne fra projektet med i betragtning ved sin vurdering.

Tiltag til at udvikle andre informationssystemer og afhjælpe informationshuller

Ind- og udrejsesystem (EES)

- Europa-Parlamentet og Rådet bør give behandlingen af lovgivningsforslagene om EES højeste prioritet, således at forslagene kan blive vedtaget inden udgangen af 2016.

Passagerlister (PNR)

- Europa-Parlamentet og Rådet bør vedtage PNR-direktivet senest i april 2016.
- Medlemsstaterne gennemfører PNR-direktivet som en hastesag, når det er blevet vedtaget.
- Kommissionen støtter dataudvekslingen mellem passagerinformationsenheder gennem standardiserede løsninger og procedurer.
- Kommissionen udarbejder et udkast til gennemførelsesafgørelse om fælles protokoller og understøttede dataformater til overførsel af PNR-data fra luftfartsselskaber til disse enheder senest tre måneder efter vedtagelsen af PNR-direktivet.

[25] Formålet med den automatiserede dataudvekslingsprocedure (ADEP) er at få et teknisk system, som giver mulighed for via et indeks at se, om der er politioplysninger om en person eller en strafferetlig efterforskning i en eller flere medlemsstater. Det automatiserede svar på en søgning i indekset vil kun angive, om der findes eller ikke findes data, altså om der er et "hit" eller ikke. Hvis der er et "hit, vil der skulle anmodes om yderligere personoplysninger via de sædvanlige kanaler for politisamarbejde.

Informationshul forud for ankomst af tredjelandsstatsborgere, der er fritaget for visumkravet

- Kommissionen vil i 2016 se nærmere på, om det er nødvendigt, teknisk gennemførligt og proportionelt at indføre et nyt EU-værktøj, for eksempel et EU-system vedrørende rejseinformation og rejsetilladelse.

Europæisk informationssystem vedrørende politiregistre (EPRIS)

- Kommissionen vil i 2016 se nærmere på, om det er nødvendigt, teknisk gennemførligt og proportionelt at indføre EPRIS.

7. INTEROPERABILITET FOR INFORMATIONSSYSTEMER

Interoperabilitet betyder, at der kan udveksles og deles information mellem informationssystemer. Der kan skelnes mellem **fire former for interoperabilitet**, som hver især rejser spørgsmål af retlig[26], teknisk og operationel art, herunder databeskyttelse:

- en fælles søgegrænseflade, hvor der simultant kan forespørges i flere informationssystemer, og hvor resultaterne kan ses kombineret på en enkelt skærm
- sammenkobling af informationssystemer, hvorved data, der er registreret i et system, automatisk kan konsulteres i et andet system
- oprettelse af en fælles biometrisk matchtjeneste, som kan understøtte forskellige informationssystemer
- et fælles dataregister for forskellige informationssystemer (kernemodul).

For at få sat gang i arbejdet med interoperabiliteten for informationssystemer på EU-plan vil Kommissionen nedsætte **en ekspertgruppe om informationssystemer og interoperabilitet** på højt niveau, med deltagelse af EU-agenturer, nationale eksperter og relevante institutionelle interessenter. Ekspertgruppen vil få til opgave at se på retlige, tekniske og operationelle aspekter af de forskellige muligheder for at opnå interoperabilitet for informationssystemer, herunder om de tilgængelige muligheder er nødvendige, teknisk gennemførlige og proportionelle, og hvilken indvirkning de kan få på databeskyttelse. Den skal se på de aktuelle mangler og videnshuller, som er forårsaget af, at informationssystemerne på europæisk plan i den grad er komplekse og fragmenterede. Den skal anlægge et bredt, alsidigt perspektiv på grænseforvaltning og retshåndhævelse og også tage hensyn til toldmyndighedernes roller, ansvar og systemer i den forbindelse. Gruppen skal i sit arbejde udnytte og samle alle relevante erfaringer, som hidtil alt for ofte er blevet indhøstet hver for sig.

Formålet hermed er at få en overordnet strategisk vision for EU's dataforvaltningsstruktur for grænsekontrol og sikkerhed og ligeledes at foreslå løsninger til, hvordan den kan gennemføres.

Ledetråden for denne proces skal være **følgende mål:**

- Informationssystemerne skal komplementere hinanden. Overlapninger skal undgås, og eksisterende overlapninger skal fjernes. Huller skal afhjælpes på passende måde.
- Der skal tilstræbes en modulær tilgang, hvor den teknologiske udvikling udnyttes fuldt ud, og som bygger på princippet om privacy by design.

[26] Under hensyn til de særlige betingelser i protokol 22 for så vidt angår Danmark og protokol 21 og 36 for så vidt angår Det Forenede Kongerige og Irland.

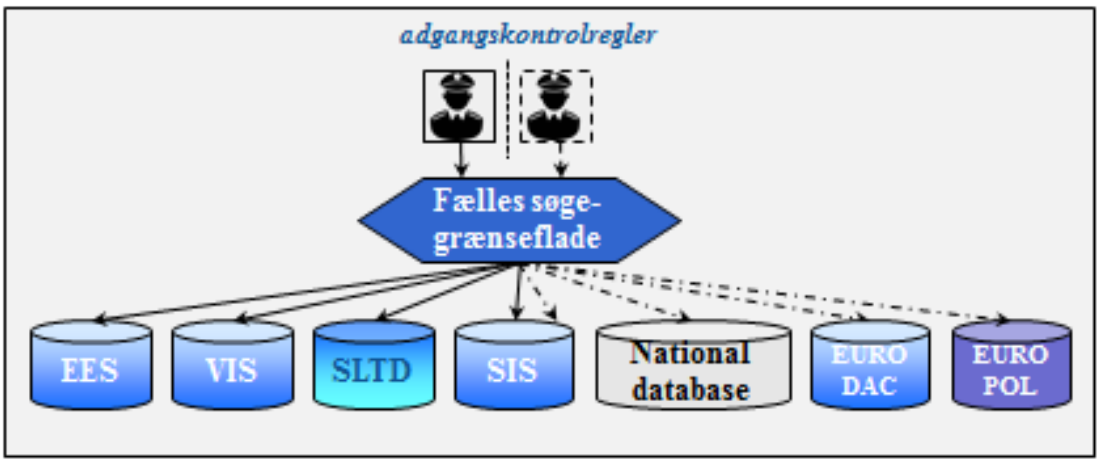
- Fuld respekt for alle grundlæggende rettigheder for både EU-borgere og tredjelandsstatsborgere skal sikres fra starten i overensstemmelse med chartret om grundlæggende rettigheder.
- Hvor det er nødvendigt og gennemførligt, skal informationssystemer sammenkobles og gøres interoperable. Det skal være lettere at foretage simultane søgninger i systemer for at sikre, at grænsevagter og politifolk har adgang til alle relevante oplysninger, når og hvis det er nødvendigt for deres respektive opgaver, uden at det ændrer ved de eksisterende adgangsrettigheder.

1. Fælles søgegrænseflade

Den første form for interoperabilitet er, at grænsevagter og politifolk **har mulighed for at forespørge i flere informationssystemer simultant, og at de kan se resultaterne kombineret på en enkelt skærm**, under fuld iagttagelse af deres adgangsrettigheder og ud fra de respektive formål. Det kræver, at der er platforme, som har en fælles søgegrænseflade, hvormed flere informationssystemer kan konsulteres simultant med en enkelt forespørgsel. Ved for eksempel at læse chippen på et rejsedokument eller at anvende biometriske data vil der med denne platform kunne forespørges i mange forskellige databasere på samme tid. Den fælles søgetilgang gælder for alle myndigheder, der har brug for at have adgang til kunne anvende data (dvs. grænsevagter, retshåndhævende myndigheder, asyltjenester) i overensstemmelse med formålsbegrænsningen og strikte regler om adgangskontrol. Der vil også kunne benyttes mobilt udstyr. Ved at indføre en fælles søgegrænseflade bliver det mindre kompliceret at anvende informationssystemerne på europæisk plan, idet grænsevagter og politifolk hermed kan forespørge i flere informationssystemer simultant gennem én procedure og i overensstemmelse med deres adgangsrettigheder.

Der er allerede flere medlemsstater, som har indført sådanne platforme med en fælles søgegrænseflade. Ud fra hvad der nu er bedste praksis, vil Kommissionen sammen med eu-LISA arbejde på at finde en standardiseret løsning til en fælles søgegrænseflade. Medlemsstaterne kan anvende EU-midler til deres nationale programmer fra Fonden for Intern Sikkerhed til at finansiere installeringen af en sådan funktion. Kommissionen vil holde nøje øje med, hvordan medlemsstaterne gør brug af denne funktion med en fælles søgegrænseflade på nationalt plan.

Figur 2 *Fælles søgegrænseflade*



Det er lettere at foretage søgning i mange centraliserede eller nationale systemer (som vist i figuren) end i decentraliserede systemer. Kommissionen og eu-LISA vil undersøge, om det også er muligt at anvende en fælles søgegrænseflade til at foretage simultane

søgninger som one-stop-shop på decentraliserede systemer som Prüm og ECRIS. Kommissionen og eu-LISA vil foretage denne analyse sammen med Ekspertgruppen for Informationssystemer og Interoperabilitet, uden ændring af eksisterende adgangsrettigheder.

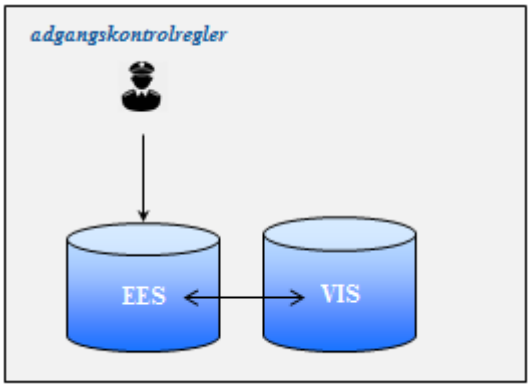
2. Sammenkobling af informationssystemer

En anden form for interoperabilitet er sammenkoblingen af informationssystemer. Det betyder, at forskellige systemer eller databaser vil kunne "tale med hinanden" teknisk set. **Data, der er registreret i ét system vil automatisk kunne konsulteres af et andet system på et centralt niveau**. Det kræver, at systemerne er teknisk kompatible, og at de dataelementer, der er lagret i disse systemer (f.eks. fingeraftryk), skal være interoperable. Ved hjælp af sammenkobling vil mængden af data, der cirkulerer på kommunikationsnet og sendes gennem nationale systemer, kunne mindskes.

Sammenkobling kræver, at der er passende databeskyttelsesforanstaltninger og strikte regler om adgangskontrol. Med den politiske enighed, som medlovgiverne nåede frem til i december 2015 om databeskyttelsesreformen, vil der kunne indføres en moderne databeskyttelsesramme for hele EU, som vil indeholde disse beskyttelsesforanstaltninger. Det er vigtigt, at medlovgiverne vedtager den generelle forordning om databeskyttelse og direktivet om databeskyttelse snarest muligt.

Begrebet sammenkobling er indbygget i det kommende EES-system. Det kommende EES vil kunne kommunikere direkte med VIS på centralt niveau og ligeledes omvendt. Det er vigtigt for at kunne afhjælpe den nuværende fragmentering i EU's struktur til dataforvaltning for grænsekontrol og indre sikkerhed, såvel som for hertil knyttede problemer. Med den automatiserede krydskontrol vil medlemsstaterne undgå at skulle forespørge i VIS ved grænsekontrol, og det vil mindske kravene til vedligeholdelse og gøre systemerne mere funktionsdygtige.

Figur 3 *Sammenkobling af systemer: eksempel med EES/VIS*



Som det næste vil Kommissionen og eu-LISA analysere, om sammenkoblingen på centralt niveau mellem det kommende EES og VIS kan udvides til at omfatte SIS, og om der kan etableres sammenkobling mellem EURODAC og SIS. Kommissionen og eu-LISA vil foretage denne analyse sammen med Ekspertgruppen for Informationssystemer og Interoperabilitet.

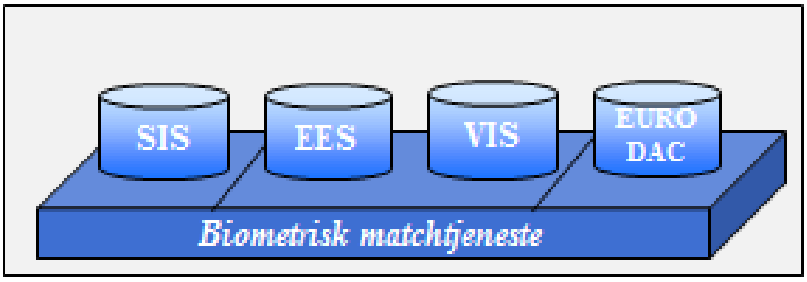
3. Fælles biometrisk matchtjeneste

En tredje form for interoperabilitet er inden for biometriske identifikatorer. Når fingeraftryk for eksempel bliver indsamlet på et konsulat i en medlemsstat med et særligt udstyr, er det af afgørende betydning, at disse aftryk kan matches gennem VIS ved en grænsestation i en anden medlemsstat, der anvender udstyr af en anden type. Det samme

krav gælder for fingeraftrykssøgninger i andre systemer: biometriske prøver skal opfylde mindstekrav til kvalitet og format, for at denne form for interoperabilitet kan fungere uden problemer.

På systemniveau gør interoperabiliteten af biometriske identifikatorer det muligt at anvende en fælles biometrisk matchtjeneste for flere informationssystemer, hvor reglerne om beskyttelse af personoplysninger respekteres, ved at dataene er opdelt i forskellige kategorier, med særskilte regler for adgangskontrol for hver kategori af data[27]. Med sådanne fælles tjenester kan der opnås betydelige finansielle, vedligeholdelsesmæssige og driftsmæssige fordele.

Figur 4 *Fælles biometrisk matchtjeneste*



Kommissionen og eu-LISA vil analysere, om det er nødvendigt og teknisk gennemførligt at oprette en fælles biometrisk matchtjeneste for alle relevante informationssystemer. Kommissionen og eu-LISA vil foretage denne analyse sammen med Ekspertgruppen for Informationssystemer og Interoperabilitet.

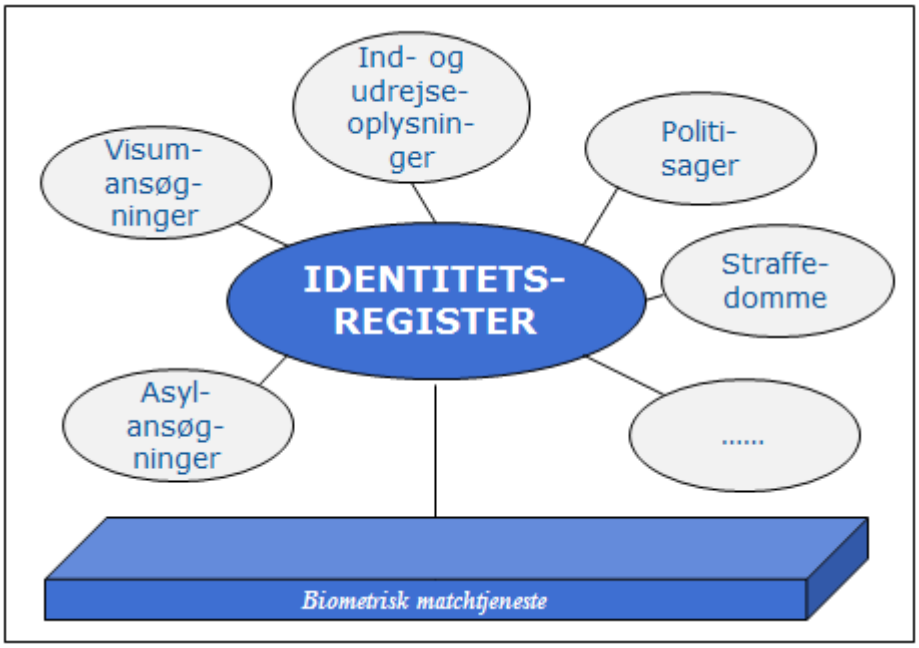
4. Fælles dataregister

Den mest ambitiøse, langsigtede tilgang til interoperabilitet vil være et **fælles dataregister på EU-plan for forskellige informationssystemer**. Det fælles register vil være et kernemodul, som indeholder basale data (alfanumeriske og biometriske data), mens andre dataelementer og specifikke egenskaber ved de forskellige informationssystemer (f.eks. visumdata) vil blive lagret i specifikke moduler. Kernemodulen og de specifikke moduler vil blive sammenkoblet for at forbinde de respektive datasæt. Det vil give en **modulær og integreret identitetsforvaltning for grænser og sikkerhed**. Det må sikres, at der er overensstemmelse med databeskyttelsesreglerne, f.eks. ved at dataene opdeles i kategorier, hvor der er seperate adgangskontrolregler for hver kategori af data.

Med oprettelsen af et fælles dataregister vil den nuværende fragmentering i EU's struktur til dataforvaltning for grænsekontrol og sikkerhed kunne overvindes. Denne fragmentering er i modstrid med princippet om dataminimering, da den resulterer i, at de samme data bliver lagret flere gange. Med det fælles register vil det, hvor det er nødvendigt, være muligt at se forbindeler og at få et overordnet billede ved at kombinere individuelle dataelementer, der er lagret i forskellige informationssystemer. Det vil dermed udfylde de nuværende videnshuller og belyse blinde pletter for grænsevagter og politifolk.

[27] Kan sammenlignes med, at én fysisk filserver deles af en lang række brugere, hvor hver enkelt bruger har specifikke adgangsrettigheder til kun bestemte foldere.

***Figur 5** Fælles dataregister*



Den eventuelle oprettelse af et fælles dataregister på EU-plan rejser vigtige spørgsmål om definition af formål, nødvendighed, teknisk gennemførlighed og proportionalitet for den heraf følgende databehandling. Det vil kræve en fuldstændig revision af den retlige ramme for de forskellige informationssystemer og vil være et mål, der kun kan nås på lang sigt. Ekspertgruppen for Informationssystemer og Interoperabilitet vil se på de retlige, tekniske og operationelle spørgsmål i forbindelse med et fælles dataregister, herunder spørgsmål om databeskyttelse.

For alle de fire former for interoperabilitet, der er nævnt ovenfor (fælles søgegrænseflade, sammenkobling af systemer, fælles biometrisk matchtjeneste og fælles dataregister), er det nødvendigt, at de data, der lagres i forskellige informationssystemer eller moduler, er kompatible. For at opnå dette er det vigtigt at arbejde hen imod et **ensartet meddelelsesformat** (UMF), for at der kan skabes en fælles standard for alle relevante informationssystemer[28].

Tiltag for interoperabilitet for informationssystemer

- Kommissionen opretter en **ekspertgruppe for informationssystemer og interoperabilitet** med deltagelse af EU-agenturer, medlemsstaterne og relevante interessenter, der skal se nærmere på de retlige, tekniske og operationelle aspekter af øget interoperabilitet for informationssystemer, herunder om de tilgængelige muligheder er nødvendige, teknisk gennemførlige og proportionelle, og hvilken indvirkning de vil få på databeskyttelse.

[28] Kommissionen har støttet den fortsatte udvikling af ensartede meddelelsesformater i meddelelsen fra 2012 om den europæiske informationsudvekslingsmodel (EIXM) og giver for øjeblikket støtte til det tredje UMF-pilotprojekt med henblik på at få indført en fælles standard for alle relevante databaser, der skal benyttes på nationalt plan (i medlemsstaterne), på EU-plan (for de centrale systemer og af agenturerne) og på internationalt plan (Interpol).

Fælles søgegrænseflade

- Kommissionen og eu-LISA hjælper medlemsstaterne med at operette en fælles søgegrænseflade til at forespørge i centrale systemer.
- Kommissionen og eu-LISA ser sammen med ekspertgruppen nærmere på, om fælles søgegrænseflader vil kunne anvendes til at foretage simultane one-stop-shop søgninger i alle relevante systemer uden ændring af eksisterende adgangsrettigheder.

Sammenkobling af informationssystemer

- Kommissionen og eu-LISA analyserer sammen med ekspertgruppen, om sammenkoblingen mellem centraliserede informationssystemer vil kunne fremmes yderligere, ud over den allerede foreslåede sammenkobling mellem ind- og udrejsesystemet og visuminformationssystemet.

Biometrisk matchtjeneste

- Kommissionen og eu-LISA analyserer sammen med ekspertgruppen, om det er nødvendigt og teknisk gennemførligt at oprette en fælles biometrisk matchtjeneste for alle relevante informationssystemer.

Fælles dataregister (kernemodul)

- Kommissionen og eu-LISA ser sammen med ekspertgruppen nærmere på de retlige, tekniske, operationelle og finansielle indvirkninger af den mere langsigtede udvikling af et fælles dataregister.
- Kommissionen og eu-LISA går med i det igangværende arbejde med et globalt ensartet meddelelsesformat for alle relevante informationssystemer.

8. KONKLUSION

Med denne meddelelse lanceres en drøftelse af, hvordan informationssystemerne i EU kan være med til at forbedre grænseforvaltning og indre sikkerhed, med udgangspunkt i signifikante synergier mellem de europæiske dagsordener om sikkerhed og om migration. Der er allerede en række informationssystemer, som giver grænsevagter og politifolk relevante oplysninger, men disse systemer er ikke perfekte. EU står over for udfordringen med at får opbygget en stærkere og mere intelligent forvaltningsstruktur, som er fuldt ud i overensstemmelse med de grundlæggende rettigheder, navnlig beskyttelse af personoplysninger og princippet om formålsbegrænsning.

Hvis der er huller i EU's dataforvaltningsstruktur, skal der tages fat herom. Kommissionen har sammen med denne meddelelse forelagt et forslag til et ind- og udrejsesystem, som bør vedtages som et hasteanliggende. Det er også nødvendigt at få vedtaget passagerlistedirektivet i de kommende uger. Forslaget om en europæisk grænse- og kystvagt bør vedtages inden sommeren. Sideløbende hermed vil Kommissionen fortsætte med at styrke og om nødvendigt strømline eksisterende systemer, for eksempel udvikle et automatiseret fingeraftryksidentifikationssystem til Schengeninformationssystemet.

Det er nødvendigt, at medlemsstaterne gør fuld brug af de eksisterende informationssystemer og opretter de nødvendige tekniske tilkoblinger til alle informationssystemer og databaser, sådan som de er retligt forpligtede til. De eksisterende mangler, navnlig i Prümrammen, må straks afhjælpes. Denne meddelelse åbner op for en drøftelse af og starter en proces, som skal afhjælpe systemiske huller og brister, men det er medlemsstaterne, der snarest muligt skal afhjælpe vedvarende problemer med indlæsningen i EU-databaser og udvekslingen af oplysninger i Unionen.

For at der kan ske en strukturel forbedring af EU's dataforvaltningsstruktur for grænsekontrol og sikkerhed, sætter denne meddelelse gang i en proces, der skal føre til interoperabilitet for informationssystemerne. Kommissionen vil operette en ekspertgruppe for informationssystemer og interoperabilitet, som skal tage sig af de retlige, tekniske og operationelle aspekter ved de muligheder, der er for at opnå interoperabilitet for informationssystemerne og afhjælpe mangler og huller. På grundlag af de resultater, som ekspertgruppen når frem til, vil Europa-Kommissionen fremlægge flere konkrete ideer for Europa-Parlamentet og Rådet, der kan danne grundlag for en fælles drøftelse af, hvad der videre skal ske. Kommissionen vil også indhente input fra Den Europæiske Tilsynsførende for Databeskyttelse og fra nationale databeskyttelsesmyndigheder, som mødes i Artikel 29-Gruppen.

Målet må være at få udviklet en fælles strategi, som kan gøre dataforvaltningen i EU mere effektiv og mere virkningsfuld under fuld iagttagelse af kravene om databeskyttelse, for bedre at beskytte de ydre grænser og fremme den indre sikkerhed, hvilket er til fordel for alle borgere.

BILAG 1: FORKORTELSER

API	Forhåndsinformation om passagerer
AFIS	Automatiseret fingeraftryksidentifikationssystem: system, hvormed fingeraftryk kan tages, lagres, sammenlignes og verificeres.
CIS	Toldinformationssystem
ECRIS	Europæisk informationssystem vedrørende strafferegistre
EES	(foreslået) Ind- og udrejsesystem
EIXM	Europæisk informationsudvekslingsmodel
EIS	Europols informationssystem
EPRIS	Europæisk informationssystem vedrørende politiregistre
EURODAC	Europæisk fingeraftrykssystem
EUROPOL	Den Europæiske Politienhed (Den Europæiske Unions Agentur for Retshåndhævelse)
ETIAS	(muligt) EU-system vedrørende rejseinformation og rejsetilladelse
eu-LISA	Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed
FIND	Interpols faste netværksdatabase
FRONTEX	Det Europæiske Agentur for Forvaltning af det Operative Samarbejde ved de Ydre Grænser for Medlemsstaterne i Den Europæiske Union
iARMS	(Interpols) system til registrering og sporing af ulovlige skydevåben
INTERPOL	Den Internationale Kriminalpolitiorganisation
MIND	Interpols mobile netværksdatabase
PIU	Passagerinformationsenhed: enhed, der oprettes i hver enkelt medlemsstat, og som skal modtage PNR-dataene fra luftfartselskaberne
PNR	Passagerlister
Prüm	Politisamarbejdsmekanisme til udveksling af oplysninger om DNA, fingeraftryk og data fra køretøjsregistre
SafeSeaNet	Europæisk platform til udveksling af maritime data mellem medlemsstaternes søfartsmyndigheder
SBC	Schengengrænsekodeksen
SIENA	Netværksprogram til sikker informationsudveksling
SIS	Schengeninformationssystem (til tider omtalt som 2. generation – SIS II)
SLTD	(Interpols) database over stjålne og bortkomne rejsedokumenter
sTESTA	sikrede transeuropæiske telematiktjenester mellem administrationer (skal opgraderes til TESTA-NG (næste generation))
UMF	Uniform Message Format: format for meddelelser, som muliggør kompatibilitet mellem informationssystemer
VIS	Visuminformationssystemet
VRD	Data fra køretøjsregistre

BILAG 2: OPGØRELSE OVER EKSISTERENDE INFORMATIONSSYSTEMER TIL GRÆNSEFORVALTNING OG RETSHÅNDHÆVELSE

1. Schengeninformationssystemet (SIS)

SIS er den største og mest anvendte platform til udveksling af oplysninger om immigration og retshåndhævelse. Det er et centraliseret system, som anvendes af 25 EU-medlemsstater[29] og fire Schengenassocierede lande[30], og det indeholder for øjeblikket 63 millioner indberetninger. De bliver indført og konsulteret af kompetente myndigheder som politi, grænsekontrol og immigration. Det indeholder oplysninger om tredjelandsstatsborgere, som har forbud mod at indrejse i eller opholde sig i Schengenområdet, og om tredjelandsstatsborgere, som er eftersøgt eller forsvundet (herunder børn), samt om efterlyste genstande (våben, køretøjer, identitetsdokumenter, industriudstyr osv.). SIS adskiller sig fra andre informationsdelingsinstrumenter ved, at oplysningerne heri er suppleret med instrukser om konkrete tiltag, som de ansatte på stedet skal iværksætte, for eksempel anholdelse eller beslaglæggelse.

Det er obligatorisk at foretage kontrol i SIS ved behandling af visa til kortvarigt ophold, ved grænsekontrol af tredjelandsstatsborgere og ikkesystematisk kontrol af EU-borgere[31] og andre personer, der har ret til fri bevægelighed. Desuden skal al politikontrol i området også omfatte automatisk kontrol i SIS.

2. Visuminformationssystemet (VIS)

VIS er et centraliseret system til udveksling af data om visa til kortvarigt ophold mellem medlemsstaterne. Det behandler data og afgørelser vedrørende ansøgninger om visum til kortvarigt ophold til at besøge eller til at passere gennem Schengenområdet. Alle Schengenstaternes konsulater (omkring 2000) og alle deres ydre grænseovergangssteder (i alt ca. 1800) er blevet tilkoblet systemet.

VIS indeholder data om visumansøgninger og -afgørelser og om, hvorvidt udstedte visa er blevet tilbagekaldt, annulleret eller forlænget. Det indeholder for øjeblikket data om 20 millioner visumansøgninger, og i perioder med spidsbelastning behandles over 50 000 transaktioner i timen. Hver visumansøger giver detaljerede biografiske oplysninger, et digitalt foto og ti fingeraftryk. Det er således et pålideligt middel til at verificere identiteten for visumansøgere, til at vurdere mulige tilfælde af irregulær migration og sikkerhedsrisici og til at forhindre "visumshopping".

Ved grænseovergangssteder eller inden for medlemsstaternes område benyttes VIS til at verificere identiteten på visumindehavere ved, at deres fingeraftryk sammenlignes med de fingeraftryk, der er lagret i VIS. Det giver sikkerhed for, at den person, der ansøgte om visummet, er den samme, som den der krydser grænsen. Ved en fingeraftrykssøgning i VIS er det også muligt at identificere en person, som har ansøgt om et visum inden for de seneste fem år, og som måske ikke har identitetsdokumenter på sig.

[29] Alle, undtagen Irland, Cypern, Kroatien.
[30] Schweiz, Liechtenstein, Norge, Island.
[31] Denne regel er ved at blive ændret med Kommissionens forslag COM/2015/0670 om ændring af Schengengrænsekodeksen.

3. EURODAC

EURODAC (det europæiske fingeraftryksystem) indeholder fingeraftryk af asylansøgere og af tredjelandsstatsborgere, der irregulært krydser Schengenområdets ydre grænser. Dets primære formål for øjeblikket er at fastslå, hvilket EU-land der er ansvarligt for behandlingen af en asylansøgning, som fastsat i Dublinforordningen. Det er tilgængeligt ved grænseovergangssteder, men i modsætning til SIS og VIS er det ikke et grænseforvaltningssystem.

Fingeraftryk fra irregulære migranter, der kommer ulovligt ind i EU, bliver taget ved grænseovergangsstederne. De bliver lagret i EURODAC, for at en persons identitet kan verificeres i tilfælde af en kommende asylansøgning. Immigrations- og politimyndigheder kan også sammenligne fingeraftryksdata fra irregulære migranter, som bliver fundet i EU-medlemsstaterne, for at kontrollere, om de har ansøgt om asyl i en anden medlemsstat. De retshåndhævende myndigheder og Europol har også ret til at søge i EURODAC for at forhindre, opspore eller efterforske grov kriminalitet eller terrorhandlinger.

Ved at registrere fingeraftryk fra asylansøgere eller irregulære migranter i et centraliseret system vil deres sekundære bevægelser[32] inden for EU kunne identificeres og overvåges, indtil der bliver indgivet en ansøgning om international beskyttelse, eller der bliver udstedt en afgørelse om tilbagesendelse (fremover med en tilsvarende indberetning i SIS). Mere generelt er det nødvendigt med identifikation og overvågning af irregulære migranter for at sikre, at myndighederne i deres oprindelsesland kan udstede nye dokumenter, hvorved det bliver lettere at tilbagesende dem.

4. Stjålne og bortkomne rejsedokumenter (SLTD)

Interpols database over stjålne og bortkomne rejsedokumenter (SLTD) er en central database over pas og andre rejsedokumenter, som af de udstedende myndigheder er meldt stjålet eller bortkommet til Interpol. Den indeholder oplysninger om stjålne blankopas. Rejsedokumenter, der er meldt bortkommet eller stjålet til myndighederne i lande, der deltager i SIS, indlæses både i SLTD og i SIS. I SLTD er er også data om rejsedokumenter, som er indlæst af lande, der ikke deltager i SIS (Irland, Kroatien, Cypern og tredjelande).

Som anført i Rådets konklusioner fra den 9. og den 20. november 2015 og i Kommissionens forslag af 15. december 2015 til en forordning om en målrettet revision af Schengengrænsekodeksen[33] vil rejsedokumenter for alle tredjelandsstatsborgere og for personer, der har ret til fri bevægelighed, skulle verificeres i SLTD. Alle grænsekontrolposter skal være tilkoblet SLTD. Derudover vil søgninger i SLTD i indenlandsk retshåndhævelsesøjemed give yderligere sikkerhedsfordele.

5. Forhåndsinformation om passagerer (API)

Formålet med API er at indsamle oplysninger om en persons identitet, inden denne person går om bord på et fly til EU, og at identificere irregulære migranter ved deres ankomst. API-data er oplysninger fra et rejsedokument og giver den rejsendes fulde navn, fødselsdato, nationalitet, antal og type af rejsedokumenter samt oplysninger om

[32] For eksempel flygtninge, der ankommer til Grækenland, men ikke har til hensigt at ansøge om asyl i Grækenland, men at rejse videre til andre medlemsstater over land.

[33] COM(2015) 670 final, forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EF) nr. 562/2006 for så vidt angår en styrkelse af kontrollen i relevante databaser ved de ydre grænser.

grænseovergangssteder mellem afrejse og indrejse såvel som befordringsdetaljer. API-data, der vedrører passageren, indsamles sædvanligvis ved check-in.

Oplysninger før ankomst i forbindelse med transport ad søvejen skal som fastsat i konventionen om lettelse af international samfærdsel ad søvejen indgives 24 timer før skibets forventede ankomst. Direktiv 2010/65/EU[34] har bestemmelse om elektonisk overførsel af data via en enkel portal, der forbinder SafeSeaNet, e-told og andre elektroniske systemer.

Der er ikke noget centralt EU-system til registrering af API-data.

6. Europols informationssystemer

Europols informationssystem (EIS) er en centraliseret database med strafferetlige oplysninger til brug for efterforskning. Det kan anvendes af medlemsstaterne og Europol til at lagre og forespørge data om grov kriminalitet og terrorisme. De oplysninger, der er lagret i EIS, er data over personer, identitetsdokumenter, biler, våben, telefonnumre, e-mails, fingeraftryk, DNA og cyberkriminalitetsrelaterede oplysninger, som kan kobles til hinanden på forskellige måder for at få et mere detaljeret og struktureret billede af en forbrydelse. EIS understøtter samarbejde omkring retshåndhævelse og er ikke tilgængeligt for grænsekontrolmyndigheder.

Informationsudvekslingen sker gennem SIENA[35]-platformen, som er et netværk til sikker elektronisk kommunikation mellem Europol, forbindelseskontorerne, Europols nationale enheder, udpegede kompetente myndigheder (som toldvæsenet, kontorer for inddrivelse osv.) og berørte tredjeparter.

Fra maj 2017 vil der gælde en ny retlig ramme for Europol. Hermed vil der for Europol kunne opnås en bedre operationel kapacitet til at foretage analyser og til bedre at kunne identificere forbindelser mellem tilgængelige oplysninger.

7. Prümrammen

Prümrammen er baseret på en multilateral aftale mellem medlemsstaterne[36], som gør det er muligt at udveksle DNA, fingeraftryk og data fra køretøjsregistre (VRD). Konceptet er baseret på sammenkoblingen af et nationalt system til de nationale systemer i alle andre medlemsstater, således at det bliver muligt at foretage krydssøgning på afstand. Hvis en søgning giver en positiv match i en anden medlemsstats database, udveksles detaljerne i den positive match gennem bilaterale udvekslingsmekanismer.

8. Det europæiske informationssystem vedrørende strafferegistre (ECRIS)

ECRIS er et elektronisk system til udveksling af oplysninger om tidligere domme, som er afsagt i straffesager over for en bestemt person af straffedomstole i EU, med henblik på straffesager over for en person og, i fald det er tilladt ifølge national lovgivning, med andre formål. Domsmedlemsstaterne skal meddele domme mod en statsborger fra en anden medlemsstat til den medlemsstat, hvor vedkommende er statsborger. Den medlemsstat, hvor vedkommende er statsborger, skal lagre disse oplysninger og kan

[34] Europa-Parlamentets og Rådets direktiv 2010/65/EU af 20. oktober 2010 om meldeformaliteter for skibe, der ankommer til eller afgår fra havne i medlemsstaterne, og om ophævelse af direktiv 2002/6/EF.

[35] Netværksprogram til sikker informationsudveksling.

[36] Prümkonventionen af 2005. Konventionen blev integreret i EU-lovgivningen i 2008 ved Rådets afgørelse 2008/615/RIA.

dermed give ajourførte oplysninger om tidligere straffedomme over sine statsborgere efter anmodning, uanset hvor i EU dommene er blevet afsagt.

ECRIS giver også mulighed for at udveksle oplysninger om domme over for tredjelandsstatsborgere og statsløse personer. De udpegede centrale myndigheder i hver medlemsstat fungerer som kontaktpunkter i ECRIS-netværket og tager sig af alt, såsom meddele, lagre, anmode om og give oplysninger om tidligere domme.