KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 24.11.2005
KOM(2005) 597 endelig

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

om øget effektivitet, kompatibilitet og synergi blandt europæiske databaser inden for retlige og indre anliggender

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

om øget effektivitet, kompatibilitet og synergi blandt europæiske databaser inden for retlige og indre anliggender

1. BAGGRUND

I deres bestræbelser på at bekæmpe terror og styrke den interne sikkerhed har både Det Europæiske Råd og Rådet for Den Europæiske Union ved flere lejligheder opfordret Kommissionen til at fremsætte forslag om øget effektivitet, kompatibilitet og synergi blandt europæiske databaser (erklæring af 25. marts 2004 om bekæmpelse af terrorisme[1], Haag-programmet[2], Rådets erklæring af 13. juli 2005 efter terrorangrebene i London).

Det Europæiske Råd og Rådet har også gentagne gange understreget betydningen af at anvende biometri i databaser og rejsedokumenter for at styrke sikkerhedsniveauet i Den Europæiske Union.

2. DEFINITIONER OG FORMÅL MED DENNE MEDDELELSE

2.1. Formålet med denne meddelelse

Den baggrund, som denne meddelelse er udarbejdet på – kampen mod terrorisme og forbrydelser – antyder, at formålet er mere vidtgående end at øge muligheden for kompatibilitet og synergi for informationsteknologiske (it) systemer inden for retlige og indre anliggender.

Formålet med denne meddelelse er at fokusere på, hvordan disse systemer - ud over deres nuværende formål - mere effektivt kan understøtte politikken i forbindelse med fri bevægelighed for personer og medvirke til at bekæmpe terrorisme og alvorlige forbrydelser.

Der skal findes en nøje balance mellem disse mål og beskyttelsen af grundlæggende rettigheder (især beskyttelse af persondata), som er knæsat i den europæiske konvention om menneskerettigheder og Den Europæiske Unions charter om grundlæggende rettigheder. Det må heller ikke glemmes, at it-systemer kan anvendes til at beskytte og styrke individets grundlæggende rettigheder.

Denne meddelelse lægger op til dybtgående debat om it-systemers form og opbygning på længere sigt. Ved at kortlægge mulige scenarier, hvoraf nogle har vidtrækkende ambitioner og konsekvenser, skal meddelelsen ikke foregribe resultatet af en grundig debat ved at fremsætte konklusioner om, hvorvidt, hvornår og under

---

[1] Rådet for Den Europæiske Union 7906/04, erklæring om bekæmpelse af terrorisme af 29. marts 2004.

[2] Haag-programmet til styrkelse af frihed, sikkerhed og retfærdighed i Den Europæiske Union af 10. maj 2005.

hvilke omstændigheder disse scenarier skal anvendes. På grund af meddelelsens politiske og strategiske karakter indeholder den ikke en detaljeret vurdering af juridiske[3], tekniske, organisatoriske eller samfundsmæssige konsekvenser af de mulige løsninger. Før der tages lovgivningsmæssige initiativer, skal der udføres grundige konsekvensanalyser, især hvad angår proportionalitetsprincippet. I sådanne analyser skal der ligeledes tages stilling til konsekvenserne for andre nuværende eller påtænkte samarbejdsmetoder mellem de myndigheder, der er ansvarlige for den interne sikkerhed (f.eks. gennem Europol).

Denne meddelelse indledes med en kortfattet beskrivelse af situationen i dag med de eksisterende og fremtidige fælleseuropæiske it-systemer og de huller, der er konstateret i bestræbelserne på at nå de nuværende mål. Derefter vil der blive fremlagt scenarier for brug af disse systemer på mere effektiv vis og med henblik på at skabe eventuelle systemer i fremtiden. Endelig undersøges det, hvorvidt de tekniske og driftsmæssige muligheder står i rimeligt forhold til behovet for at beskytte individets rettigheder.

I denne meddelelse stilles ikke forslag om yderligere kompatibilitet eller synergi på nationalt niveau. Selv om foranstaltninger på europæisk niveau må forventes at have indflydelse på de nationale systemer, er det medlemsstaternes opgave at analysere, hvordan de nationale systemer kan arbejde bedre sammen.

2.2. Begreber

Før der gives flere detaljer, bør der skabes klarhed om følgende begreber:

Ved *"kompatibilitet"* forstås IT-systemers og deres understøttede forretningsprocedurers evne til at udveksle data og muliggøre deling af oplysninger og viden[4]. Denne "kompatibilitet" er et teknisk, ikke juridisk eller politisk, begreb. Dette spørgsmål berører ikke, om dataudvekslingen er lovlig, politisk mulig eller krævet[5].

"Konnektivitet" er en generisk betegnelse for forbindelsesanordninger med dataoverførsel for øje.

"Synergi" omfatter tekniske, økonomiske og organisatoriske elementer. Teknisk set betyder "synergi" et gensidigt fordelagtigt sammenfald af forskellige elementer. Økonomisk set betyder den en stigning i værdien af aktiver eller stordriftsfordele. I organisatorisk sammenhæng betyder "synergi" samling af tidligere adskilte ressourcer eller strømlining af den eksisterende organisation, så dens effektivitet øges.

---

3 Heri indgår medvirken af de lande, der ikke (fuldt ud) deltager i Schengen-samarbejdet.

4 European Interoperability Framework for Pan-European eGovernment Services, Kontoret for De Europæiske Fællesskabers Officielle Publikationer, 2004, punkt 1.1.2.

5 Detaljerne om, hvordan organisationer aftaler at arbejde sammen rent teknisk ved dataudveksling, fastlægges normalt i en rammeaftale om kompatibilitet, der kan defineres som et sæt standarder og retningslinjer, jf. European Interoperability Framework for Pan-European eGovernment Services, Kontoret for De Europæiske Fællesskabers Officielle Publikationer, 2004, punkt 1.1.2.

"Rådighedsprincippet" betyder, at de myndigheder, der har ansvar for intern sikkerhed i én medlemsstat eller Europol-tjenestemænd, som har behov for oplysninger ved udførelsen af deres opgaver, bør indhente disse oplysninger fra en anden medlemsstat, hvis de er til rådighed på det pågældende sted.

3. STATUS OG FORMÅL MED NUVÆRENDE OG FREMTIDIGE IT-SYSTEMER

Denne meddelelse fokuserer på SIS II, VIS og EURODAC, som er de systemer, der især er blevet fremhævet af Det Europæiske Råd og Rådet for Den Europæiske Union i deres mandat. Hvert system har en særlig målsætning. De personlige data, som de behandler, er ikke nødvendigvis de samme, da de er begrænset til dem, som er relevante for det enkelte systems specifikke målsætning. Ligeledes er det ikke altid de samme myndigheder, som har adgang til data.

3.1. SIS II

Anden generation af "Schengen Information System" (SIS II) vil gøre det lettere at rejse over grænserne i det udvidede EU, uden at dette går ud over sikkerheden. Det giver myndighederne i medlemsstaterne mulighed for at samarbejde ved at udveksle oplysninger, så de kan etablere et område uden indre grænsekontrol. De udvekslede oplysninger skal bruges til kontrol af personer ved de ydre grænser eller på det nationale territorium samt ved udstedelse af pas, visum og opholdstilladelse og derudover til politimæssigt og retligt samarbejde i kriminalsager[6].

3.2. VIS

"Visa Information System" (VIS) vil være til fordel for folk, der rejser i god tro ved at forbedre procedurerne for visumudstedelse. Det vil forbedre styringen af den fælles visumpolitik og samarbejdet mellem konsulater med henblik på at: forhindre trusler mod den indre sikkerhed og uensartede kriterier for udstedelse af visum, lette kampen mod svig, medvirke til identifikation og udvisning af personer med ulovligt ophold og lette anvendelsen af Dublin II-forordningen[7].

Den 7. marts 2005 konkluderede Rådet, at de myndigheder, der er ansvarlige for intern sikkerhed, burde havde adgang til VIS. Kommissionen vil fremsætte et forslag om at give både Europol og myndighederne med ansvar for indre sikkerhed adgang til VIS til klart definerede formål.

3.3. EURODAC

Formålet med EURODAC er at bistå med at fastslå, hvilke medlemsstater der er ansvarlige efter Dublin II-forordningen og at lette brugen heraf. EURODAC er nødvendig for at kunne sikre det europæiske asylsystems effektivitet.

---

6 Betingelserne for behandling af persondata vil blive fastlagt i retsinstrumenterne om regulering af SIS II.

7 Rådets forordning (EF) nr. 343/2003 af 18. februar 2003 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning, der er indgivet af en tredjelandsstatsborger i en af medlemsstaterne, EFT L 50 af 25.2.2003.

4. KONSTATEREDE MANGLER

Selv om SIS II, VIS og EURODAC er omdrejningspunktet for denne meddelelse, drøftes der også andre spørgsmål i forbindelse med kampen mod terrorisme og kriminalitet.

4.1. Underudnyttelse af de nuværende systemer

De nuværende systemer udnyttes endnu ikke fuldt ud. Dette gælder f.eks. visse advarselskategorier i SIS, såsom advarsler, der udsendes ved diskret overvågning eller specifik kontrol, der anvendes begrænset og uensartet. Øget og mere konsekvent brug af disse advarsler kan styrke kampen mod terrorisme. Ud over de data, der bearbejdes i fælles systemer, bruger mange medlemsstater særskilte lister til samme formål, for eksempel ved afvisning af indrejse, hvilket medfører dobbeltarbejde for mange medlemsstater.

EURODAC-forordningen er ligeledes underudnyttet. Selv om EURODAC-forordningen forpligter medlemsstaterne til at tage fingeraftryk af alle personer over 14, som ulovligt krydser deres grænser, og som ikke kan afvises, udgør den datamængde, der sendes til EURODAC en overraskende lille brøkdel af den samlede migrationsstrøm.

4.2. Begrænsninger ved alfanumeriske forespørgsler

En alfanumerisk forespørgsel lykkes kun, hvis oplysningerne er forholdsvis nøjagtige. Hvad angår personer, øges sandsynligheden for ikke at opnå det rigtige resultat med databasens størrelse. Desto flere navne, der er i databasen, desto sværere er det at finde en person, og desto større er sandsynligheden for at fejlidentificere en person. Fejlagtige oplysninger (f.eks. et navn eller en fødselsdato fra et forfalsket dokument eller forskellige translitterationer af det samme navn) giver forkerte resultater. Derudover bliver en alfanumerisk forespørgsel med data, der ikke er unikke, mindre nøjagtig, jo flere data der lagres i databasen. Dette giver et stort antal søgeresultater, som derefter skal verificeres ved en arbejdskrævende proces, der undertiden kan være umulig at udføre, når der er tale om grænsekontrol.

4.3. Ingen fordele for rejsende i god tro

Af de personer, der ansøger om Schengen-visum, anslås ca. 20 % til at være regelmæssige rejsende, dvs. personer, der ansøger om visum til flere indrejser. For disse rejsende er der ringe muligheder for at mindske ventetiden. Hvis deres rejsedokumenter går tabt eller bliver stjålet, skal rejsende i god tro igennem en indviklet proces for at få nye rejsedokumenter.

4.4. Identifikation af ulovlige indvandrere er vanskelig

Mange ulovlige indvandrere, der pågribes, har ingen identifikation på sig eller anvender forfalskede identifikationsdokumenter. I sådanne tilfælde er identifikationsprocessen tidskrævende og kostbar. Hvis rejsedokumenterne er blevet ødelagt, har myndighederne ikke for indeværende et system, der gør det muligt for dem at kontrollere personernes identitet.

4.5. Ineffektiv anvendelse af Dublin II-forordningen

Denne forordning definerer kriterierne for, hvilken medlemsstat der er ansvarlig for at undersøge asylansøgninger. Et grundlæggende kriterium er, hvorvidt medlemsstaten har udstedt eller forlænget et visum til en asylansøger. Medlemsstaterne har for indeværende ingen effektive midler til at undersøge, hvorvidt en asylansøger har fået udstedt et visum fra en anden medlemsstat, bekræfte personens identitet eller fastslå visummets gyldighed.

4.6. Ingen mulighed for at anvende asyl-, indvandrings- og visumdata til interne sikkerhedsformål

I forbindelse med målsætningen om at bekæmpe terrorisme og forbrydelser finder Rådet nu, at de interne sikkerhedsmyndigheders manglende adgang til VIS-data er et problem. Dette samme kan hævdes om samtlige SIS II-data om indvandring og om EURODAC-data. De retshåndhævende myndigheder betragter nu dette som en alvorlig mangel ved identifikationen af personer, der mistænkes for alvorlige forbrydelser.

4.7. Ikke alle kategorier af statsborgere fra tredjelande kontrolleres

VIS dækker for tiden kun statsborgere fra tredjelande med visumpligt. Kontrollen med identitet og lovlighed, for så vidt angår andre kategorier af statsborgere fra tredjelande, der hyppigt krydser grænserne, f.eks. indehavere af visa til længerevarende ophold eller opholdstilladelser eller statsborgere fra tredjelande uden visumpligt, kan også gøres mere effektiv. Dette opfatter myndighederne med ansvar for intern sikkerhed og efterretningstjenesterne som en mangel.

4.8. Ufuldstændig overvågning af ind- og udrejse, der foretages af statsborgere fra tredjelande

Selv om VIS giver mulighed for at kontrollere en ansøgers tidligere visumansøgninger og at kontrollere, om den person, der forelægger et visum ved grænsen, er den samme, som visummet er udstedt til, følger VIS ikke indrejsende statsborgere fra tredjelande med visum, og systemet følger heller ikke med i, hvorvidt statsborgere fra tredjelande rejser ud, før deres opholdsret er udløbet. Med andre ord kan hverken VIS eller for den sags skyld SIS II identificere personer med ulovligt ophold i EU.

4.9. Manglende biometriske identifikationsværktøjer

Det er et grundlæggende krav for myndigheder med ansvar for bekæmpelse af forbrydelser og terrorisme, at de skal kunne identificere personer, selv hvis der kun foreligger biometriske oplysninger, f.eks. et foto, fingeraftryk eller DNA-kode. Automated Fingerprint Identification System (AFIS) og DNA-databaser gør det muligt at foretage en sådan identificering. Da sådanne databaser nu findes i de fleste medlemsstater, arbejder Kommissionens tjenestegrene på et forslag om samkøring af nationale DNA-databaser. Kommissionen agter også at fremsætte forslag til en retsakt om fingeraftryk til næste år. På det nuværende udviklingsstadium giver SIS II kun mulighed for at indføre en advarsel, hvis der som minimum kan indføres grundlæggende alfanumeriske oplysninger i systemet. Denne mangel understreges af,

at Prüm-traktaten der blev underskrevet af syv medlemsstater den 27. maj 2005, giver mulighed for bilateral udveksling af data om fingeraftryk og DNA, indtil der er vedtaget et lignende retligt instrument på europæisk plan.

4.10. Ingen registrering af EU-borgere på europæisk plan

Identificering af EU-borgere på grundlag af rejse- og identitetspapirer bliver snart forbedret ved indførelse af biometriske identifikatorer. Da de fleste medlemsstater imidlertid vil have centralarkiv og udstedte dokumenter og biometriske identifikatorer, der forbindes med en given identitet, giver en forespørgsel til arkivet kun mulighed for at kontrollere, hvorvidt denne medlemsstat tidligere har udstedt et dokument til den samme person, men under et andet navn. Derudover er det ikke i øjeblikket muligt at foretage en forespørgsel om en person, der f.eks. er eftersøgt for terrorisme på grundlag af, om denne person tidligere har fået udstedt et rejse- eller identifikationsdokument.

Dette er ligeledes blevet konstateret som en mangel i kampen mod identitetstyveri, som vækker stadig mere bekymring blandt myndighederne med ansvar for intern sikkerhed, og det er til væsentlig skade for den europæiske økonomi.

4.11. Identificering af ulykkesofre og ukendte lig

Der findes ingen omfattende database, som giver mulighed for at identificere ulykkesofre og ukendte lig. Muligheden for at anvende en Interpol-database til dette formål er blevet drøftet i Rådet. En sådan database vil imidlertid ikke kunne dække alle tilfælde.

5. YDERLIGERE MULIG UDVIKLING

5.1. Bedre anvendelse af eksisterende systemer

Mere effektiv brug af de nuværende systemer kan først og fremmest opnås ved øget brug af de muligheder, der allerede findes: bedre kvalitetskontrol af datainput, mere sammenhæng ved input af datakategorier og øget brugervenlighed. I denne sammenhæng vil det være nyttigt med bredere og mere direkte henvendelser blandt medlemsstaterne og erfaringsudveksling. Selv om kontakterne overvejende bør ske inden for de bestående arbejdsgrupper og udvalg, vil regelmæssige brugerkonferencer også være til hjælp. Denne yderligere form for høring kan medvirke til at kortlægge, hvor der er behov for forbedringer, og resultaterne kan derefter indgå i lovgivningsprocessen og/eller det daglige arbejde.

Derudover bør medlemsstaterne sørge for en mere konsekvent indføring og brug af visse data (f.eks. SIS II-advarsler om personer, der muligvis agter at begå alvorlige forbrydelser, og EURODAC-data om personer, der krydser grænserne ulovligt m.v.).

5.2. Yderligere udvikling af eksisterende og planlagte systemer

5.2.1. Biometriske forespørgsler i SIS II

At identificere personer i databaser med millioner af forekomster er blevet muligt i EURODAC, og det vil der blive arbejdet på i VIS ved brug af biometrisk søgning,

der giver en hidtil uset nøjagtighed. Forslagene til retsinstrumenter om SIS II giver mulighed for bearbejdning af biometriske oplysninger (fotografier og fingeraftryk). Da SIS II er under udvikling, vil biometri imidlertid kun blive brugt til at bekræfte identifikationen af den eftersøgte (ved eftersøgte forstås personer, for hvem der er udsendt en advarsel, herunder personer, som bør nægtes indrejse) på grundlag af en alfanumerisk søgning.

Når det bliver muligt at foretage biometriske forespørgsler, bliver identifikationen af de eftersøgte mere nøjagtig. SIS II kommer dog kun til at indeholde biometriske oplysninger, der lovligt kan kædes sammen med en advarsel i SIS II.

5.2.2. Mere omfattende adgang til VIS og SIS II for asyl- og indvandringsmyndighederne

I de foreslåede retsakter gives asylmyndighederne adgang til VIS og SIS II. På den ene side vil VIS og SIS II indeholde data, som kan angive, at et af kriterierne til bestemmelse af den ansvarlige medlemsstat, er opfyldt: udstedelse af visum eller ulovligt ophold i en medlemsstat. På den anden side kan VIS og SIS II indeholde data, der fuldender vurderingen af en asylansøgning: visumdata kan hjælpe ved vurderingen af en asylansøgnings troværdighed, og SIS II-data indikere, om asylansøgeren er en trussel mod den offentlige orden eller den nationale sikkerhed. En forespørgsel i EURODAC, SIS II og VIS giver asylmyndighederne mulighed for at kontrollere data i de tre systemer samtidig.

Adgang til VIS og visse biometriske data i SIS II vil have væsentlig betydning for kampen mod ulovlig indvandring. Udokumenterede personer med ulovligt ophold kan let identificeres. Dette vil gøre det enklere at kontrollere, om visse personer er rejst ind på lovlig vis og at udpege, hvem der skal udvises.

5.2.3. Adgang for myndigheder med ansvar for intern sikkerhed

For så vidt angår VIS, vil Kommissionen fremlægge et udkast til en retsakt om udbredelse af adgangen for myndigheder med ansvar for intern sikkerhed med det formål at forhindre, efterforske og undersøge terrorhandlinger.

Hvad angår SIS II-data i forbindelse med nægtet indrejse, bør der lægges planer for udvidet adgang for myndigheder med ansvar for intern sikkerhed i sammenhæng med forebyggelse, opdagelse, efterforskning og undersøgelse af forbrydelser. Dette bør indgå som en del af de øvrige nuværende muligheder for bearbejdning af data om personer, som udgør en sikkerhedsrisiko. Der skal ligeledes tages stilling til specifikke spørgsmål som gensidighed med medlemsstater, der ikke fuldt ud deltager i politikken i forbindelse med fri bevægelighed for personer.

For EURODAC gælder det, at de eneste oplysninger, der kan bruges til at identificere en person, kan være de biometriske oplysninger, der findes i EURODAC, hvis den pågældende mistænkes for at have begået en forbrydelse eller en terrorhandling, men ikke står i en anden database eller kun er registreret med alfanumeriske eller ukorrekte data (f.eks. hvis personen har opgivet en forkert identitet eller anvendt falske dokumenter). Myndigheder med ansvar for intern sikkerhed kunne således tænkes at få adgang til EURODAC i veldefinerede sager, hvor der er en velbegrundet mistanke om, at en person, der har begået en alvorlig

forbrydelse, har ansøgt om asyl. Denne adgang bør ikke gives direkte, men gennem de myndigheder, der er ansvarlige for EURODAC.

Adgang til disse systemer kan også være nyttig ved identificering af ulykkesofre og ukendte lig.

5.3. Langsigtede scenarier og yderligere udvikling

5.3.1. Oprettelse af et europæisk automatiseret identifikationssystem med fingeraftryk fra kriminelle (AFIS)

Udover det forslag, der allerede er nævnt om sammenligning af DNA-profiler, kan der oprettes et europæisk AFIS, hvor alle fingeraftrykdata, der indtil nu kun har været til rådighed i de nationale AFIS-systemer, bliver samlet. Et sådant AFIS-system kan enten fungere på centraliseret europæisk plan eller som en decentraliseret løsning (med forbindelser mellem de nuværende AFIS). Det kan anvendes ved politiefterforskninger og vil være mere vidtgående end den positive/negative biometriske forespørgsel, som er skitseret for SIS II.

Også her vil der være tale om et bidrag til identificeringen af ulykkesofre og ukendte lig.

5.3.2. Oprettelse af et system for ind- og udrejse og indførelse af et forenklet system til indrejse for personer, der hyppigt krydser grænserne

Hovedformålet med et system for ind- og udrejse er, at ind- og udrejsende personer undersøges, og der indsamles oplysninger om deres indvandrings- og opholdsstatus. Ved ind- og udrejse til og fra Den Europæiske Union kan statsborgere fra tredjelande blive registreret ved brug af biometriske identifikatorer. Et sådant system for ind- og udrejse kan imidlertid ikke også omfatte EU-borgere, da dette vil være i strid med princippet om fri bevægelighed.

Spørgsmålet er, om en sådan løsning er mulig på grund af det store antal rejsende, der hver dag krydser EU's grænser. For at mindske antallet af kontroller, kan der indføres et program for kendte rejsende i god tro (dvs. pendlere) for at lette og automatisere rejserne over grænserne. Et lignende program fungerer mellem De Forenede Stater, Canada og Mexico, hvor rejsende i god tro efter at have gennemgået en særlig grundig baggrundskontrol får udstedt et særligt kort for betroede rejsende, der gør det muligt for dem at krydse grænserne ved brug af næsten fuld automatisering. Udrejseregistrering kan foregå via en procedure med selvregistrering. Incitamentet hertil er, at hvis der ikke er registreret udrejse, vil der fremover ikke blive givet tilladelse til indrejse, eller der vil kun blive givet en sådan tilladelse efter en specifik procedure.

Selv om et system for ind- og udrejse vil gøre grænsekontrollen meget mere effektiv, kræver det et omfattende organisatorisk skridt og kan derfor være risikabelt og kostbart at gennemføre. Imidlertid kan situationen tages op til overvejelse, når VIS er driftsklart.

Under alle omstændigheder vil det blive nødvendigt at gennemføre konsekvensanalyser eller lignende foranstaltninger med henblik på at vurdere forholdsmæssigheden ved dette og de andre fremlagte scenarier.

5.3.3. Europæisk(e) register/registre for rejsedokumenter og identitetskort

De fleste medlemsstater vil oprette deres egne databaser over udstedte rejsedokumenter og identitetskort, herunder biometriske identifikatorer, der er indleveret sammen med ansøgning. Disse databasers effektivitet kan øges væsentligt, hvis der etableres et register over indeks på europæisk plan. Alternativt kan der skabes forbindelse mellem de nationale databaser. Uanset hvilken løsning der bliver vedtaget, kan disse registre kun indeholde meget begrænsede datasæt (dokumentnummer og biometri), men vil give mulighed for autenticitetskontrol af hvert rejse- eller identitetsdokument, der udstedes i en medlemsstat, og ved brug af biometriske oplysninger vil man kunne fastslå identiteten af enhver person, som har fået udstedt et rejse- eller identitetsdokument.

Denne metode kan også hjælpe med at identificere ulykkesofre og ukendte lig.

5.4. Arkitektur- og organisationsændringer

Uden at foretage en detaljeret analyse af de tekniske og organisatoriske ændringer, der kræves for at kunne gennemføre de ovennævnte scenarier, skal det anføres, at udviklingen af en serviceorienteret arkitektur for europæiske it-systemer vil medvirke til at maksimere synergieffekter og begrænse investeringerne til et realistisk niveau. En serviceorienteret arkitektur er en metode til deling af funktioner på en fleksibel og omkostningseffektiv måde, uden at de eksisterende systemer skal sammensmeltes. Som et konkret eksempel kan nævnes brugen af den meget effektive fremtidige AFIS-del af VIS til levering af AFIS–relaterede tjenester (dvs. biometriske søgninger efter andre applikationer, f.eks. EURODAC eller muligvis et biometrisk pasregister). Datalagring og -flow kan stadig adskilles konsekvent.

Organisatorisk set er det en selvfølge, at hvis den daglige styring (dvs. ikke nødvendigvis ikke den strategiske eller politiske styring) af disse systemer lægges ind under en enkelt organisation, vil dette også medføre væsentlige synergieffekter. Styring af applikationer i et enkelt organisatorisk miljø er derfor en mulighed, der bør undersøges som et langsigtet mål. I forhold til målene i det foreslåede Freedom-program[8] er spørgsmålet om at overlade styringen af store it-systemer (EURODAC, SIS II, VIS) til agenturet for forvaltning af de ydre grænser på et senere tidspunkt, er en af de muligheder, der bør undersøges.

6. DE MULIGE FORANSTALTNINGERS FORENELIGHED MED MENNESKERETTIGHEDERNE, HERUNDER DATABESKYTTELSE

Hvad angår bedre identificering af eftersøgte personer, hvor lagring af persondata i databaser over kriminelle kan retfærdiggøres på baggrund af tidligere samt reelle

[8] Forslag til Europa-Parlamentets og Rådets beslutning om oprettelse af Den Europæiske Flygtningefond for perioden 2008-2013 som en del af det generelle program om solidaritet og forvaltning af migrationsstrømme.

eller formodede handlinger fra personens side (disse skal underbygges), gælder dette ikke EURODAC eller VIS. Ansøgninger om asyl eller visum giver ikke på nogen måde anledning til at antage, at en hidtil uskyldig person vil begå en forbrydelse eller en terrorhandling.

Proportionalitetsprincippet kræver derfor, at der kun vil blive søgt i disse databaser med henblik på at forebygge og undersøge alvorlige forbrydelser eller terrorhandlinger eller at identificere en gerningsmand bag eller en mistænkt for en forbrydelse eller terrorhandling, når der foreligger et tungtvejende hensyn til den offentlige sikkerhed, dvs. hvis den forbryder eller terrorist, der skal identificeres, har begået en så forkastelig handling, at det kan retfærdiggøres at søge i en database, hvor der er registreret personer med ren straffeattest. Tærsklen for myndigheder med ansvar for intern sikkerhed, der foretager forespørgsler i EURODAC, SIS II's indvandringsdata eller VIS, skal derfor altid være væsentlig højere end tærsklen for søgning i databaser over forbrydere. For at sikre fuld respekt for rettighederne i artikel 6, 7, 8, 48 og 49 i Den Europæiske Unions charter for grundlæggende rettigheder bør der således kun gives adgang i forbindelse med terrorhandlinger som defineret i Rådets rammeafgørelse 2002/475/RIA og til forbrydelser, der falder ind under Europols kompetence.

Hvad angår sammenligning af DNA-profiler, gør begrænsningen for en simpel positiv/negativ kontrol af en DNA-profil (alfanumerisk kæde af tal uden øvrige personoplysninger) det muligt at overholde proportionalitetsprincippet fuldt ud.

Proportionalitetsprincippet er særlig vigtigt, når der er tale om oprettelse af et europæisk register for rejsedokumenter og identitetskort. Det skal bemærkes, at alle relevante myndigheder for databeskyttelse, herunder de, som går ind for oprettelse af nationale registre, har henstillet til, at der ikke oprettes et europæisk register på grund af risikoen for misbrug. Oprettelse af et sådant register bør derfor kun overvejes, hvis adgangen er strengt begrænset, og hvis søgninger i dette register kan begrundes med et tungtvejende og bydende hensyn til den offentlige sikkerhed.

Sidst, men ikke mindst, gælder det for alle de mulige foranstaltninger, at de kompetente databeskyttelsesmyndigheder skal føre omfattende tilsyn. Under alle omstædigheder vil Kommissionen ved fremsættelse af eventuelle nye forslag i overensstemmelse med meddelelse KOM(2002)172[9] foretage specifikke konsekvensanalyser for at sikre de grundlæggende rettigheder.

[9] Meddelelse fra Kommissionen af 27. april 2005 KOM(2005)172 om overholdelse af charteret om grundlæggende rettigheder i Kommissionens lovgivningsforslag (Metodologi for en systematisk og stringent kontrol).