Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om forslag til Europa-Parlamentets og Rådets forordning om fastsættelse af en ramme for interoperabiliteten mellem EU-informationssystemer (grænser og visum) og om ændring af Rådets afgørelse 2004/512/EF, forordning (EF) nr. 767/2008, Rådets afgørelse 2008/633/RIA, forordning (EU) 2016/399 og forordning (EU) 2017/2226

(COM(2017) 793 final — 2017/0351 (COD))

og om forslag til Europa-Parlamentets og Rådets forordning om fastsættelse af en ramme for interoperabiliteten mellem EU-informationssystemer (politisamarbejde og retligt samarbejde, asyl og migration)

(COM(2017) 794 final — 2017/0352 (COD))

(2018/C 283/07)

Ordfører: **Laure BATUT**

Anmodning om udtalelse	Kommissionen, 18.1.2018
	Europa-Parlamentet, 28.2.2018
Retsgrundlag	Artikel 304 i traktaten om Den Europæiske Unions funktionsmåde
Kompetence	Sektionen for Beskæftigelse, Sociale Spørgsmål og Unionsborgerskab
Vedtaget i sektionen	25.4.2018
Vedtaget på plenarforsamlingen	23.5.2018
Plenarforsamling nr.	535
Resultat af afstemningen	160/3/2
(for/imod/hverken for eller imod)	

1. **Konklusioner og anbefalinger**

1.1. EØSU finder Kommissionens forslag, der sigter mod at forbedre interoperabiliteten mellem EU informationssystemer for grænser og visum samt politisamarbejde, retligt samarbejde, asyl og migration, relevant og positivt.

1.2. Denne interoperabilitet bør ifølge udvalget være et strategisk mål for EU, så det kan forblive et åbent område, der værner om de grundlæggende rettigheder og mobilitet. EU og medlemsstaterne er forpligtede til at beskytte alle menneskers liv og sikkerhed. Princippet om nonrefoulement bør overholdes fuldt ud.

1.3. Interoperabilitetsforanstaltninger vil blive bedre forstået, hvis de:

— inden for rammerne af EU's migrationsstrategi sikrer en balance mellem frihed og sikkerhed, samtidig med at magtens tredeling respekteres;

— sikrer de berørte personers grundlæggende rettigheder, navnlig deres personoplysninger og privatliv samt deres ret til adgang til oplysninger om dem og til — gennem ukomplicerede procedurer — at få disse berigtiget og slettet inden for en rimelig frist;

— gentager, herunder i alle gennemførelsesretsakterne, kravet om, at principperne om databeskyttelse indarbejdes allerede i designfasen (indbygget privatlivsbeskyttelse);

— ikke skaber nye hindringer for normal passager- og godstransport.

1.4. EØSU efterlyser procedurer og garantier med hensyn til anvendelsen af data til retshåndhævelsesformål, der skal:

— sigte mod at anvende den EU-lovgivning, der sikrer størst beskyttelse på området (den generelle forordning om databeskyttelse);

— gøre det muligt hurtigere at fastslå, hvilken medlemsstat der er ansvarlig for behandlingen af ansøgninger om international beskyttelse;

— sikre de pågældende personer ret til domstolsprøvelse ved to instanser;

— sikre — navnlig uledsagede — mindreårige, uanset om der er tale om ulovligt ophold, forfølgelse eller kriminelle personer, retten til at få et visum, opnå beskyttelse og blive integreret samt retten til at blive glemt inden for en kortere frist end voksne.

1.5. EØSU mener, at det nuværende retsgrundlag for informationssystemerne bør styrkes og tage højde for at dataindsamlingssystemerne udvikler sig. Udvalget anbefaler derfor:

— en styrkelse af sikkerheden ved eksisterende databaser og deres kommunikationskanaler;

— en evaluering af virkningerne af øget forudgående kontrol for risikostyringen;

— en kontrol og løbende evaluering af strukturen via databeskyttelsesmyndighederne (Den Europæiske Tilsynsførende for Databeskyttelse). De ansvarlige forpligtes til hvert år at forelægge en redegørelse for de beslutningstagende myndigheder og Kommissionen om sikkerheden ved interoperabilitetskomponenterne samt hvert andet år at forelægge en redegørelse om foranstaltningernes indvirkning på de grundlæggende rettigheder.

1.6. EØSU mener, at projektet bør understøttes af kompetent personale, og anbefaler:

— robuste uddannelsesprogrammer for de berørte myndigheder og eu-LISA's ansatte;

— en streng kontrol af kompetencerne hos agenturets ansatte og stillingsansøgere.

1.7. EØSU udtrykker bekymring med hensyn til finansieringen af det nye system. Overvågningen af planlægningen skal sikre, at budgettet ikke bliver sprængt, og at projektet fuldføres senest i 2029;

1.8. EØSU anbefaler, at borgerne frem til afslutningen af projektet holdes orienteret om projektets udvikling, og at de berørte personer på en letforståelig måde informeres om den kontrol, som de er underlagt. Udvalget mener, at der bør være mulighed for at stoppe hele processen, hvis frihed og grundlæggende rettigheder trues af misbrug af systemet.

2. **Indledning**

2.1. Den internationale situation i 2017 blev anset for at være ustabil, både geopolitisk og med hensyn til medlemsstaternes interne sikkerhed, og Rådet anmodede gentagne gange Kommissionen om hurtigt at iværksætte tiltag, der gør det muligt at spore personer, som betragtes som farlige og allerede er blevet registreret i en af medlemsstaterne. Det kan få afgørende betydning for sikkerheden i EU at spore deres grænsepassager, rejser og ruter.

2.2. I sin beslutning af 6. juli 2016 opfordrer Europa-Parlamentet Kommissionen til at »give de nødvendige garantier, for så vidt angår databeskyttelse«.

2.3. De her behandlede kommissionsforslag er i tråd med målsætningen om »bevarelse og styrkelse af Schengenområdet« ([1]). EU har allerede vedtaget flere forordninger og indført digitaliserede informationstjenester i forbindelse med grænsekontrol af personer og varer.

2.4. Til orientering:

— **SIS: Schengeninformationssystemet,** der er en af de ældste mekanismer. Systemet er blevet revideret og forvalter en bred vifte af varslinger vedrørende personer og varer;

([1]) COM(2017) 570 final.

— **Eurodac: europæisk system for sammenligning af fingeraftryk** fra asylansøgere og tredjelandsstatsborgere, der opholder sig ulovligt ved grænserne og i medlemsstaterne, og for fastlæggelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning (CESE 2016-02981, ordfører: José Antonio Moreno Díaz ([2]));

— **VIS: visuminformationssystem** (visumkodeksen), der forvalter visa til kortvarige ophold (CESE 2014-02932, ordførere: Antonello Pezzini og Luis Miguel Pariza Castaños ([3]));

— **EES: ind- og udrejsesystem**, der endnu ikke er vedtaget, men som efter planen skal forvalte pas- samt ind- og udrejseoplysninger for tredjelandsstatsborgere, der besøger Schengenområdet, elektronisk (CESE 2016-03098, SOC/544, ordfører: Cristian Pîrvulescu ([4]));

— **ETIAS: europæisk system for rejseoplysninger og rejsetilladelser**, der endnu ikke er vedtaget, men som skal være et omfattende automatiseret system til lagring og forudgående kontrol af oplysninger om tredjelandsstatsborgere, der er fritaget for visumpligt for rejser inden for Schengenområdet (CESE 2016-06889, SOC/556, ordfører: Jan Simons ([5]));

— **ECRIS-TCN: et europæisk informationsudvekslingssystem vedrørende strafferegistre for tredjelandsstatsborgere**, som Kommissionen har fremsat forslag til. Der er tale om et digitalt system til informationsudveksling om retsafgørelser, som er afsagt af de nationale domstole.

2.5. Man kan sammenligne en ansvarlig myndigheds nuværende midler med en smartphone med forskellige apps, der alle fungerer uafhængigt af hinanden og hver især giver adgang til »egne« oplysninger.

2.6. Bortset fra SIS har disse systemer fokus på **forvaltningen af tredjelandsstatsborgere**. Der findes seks decentrale systemer, der supplerer hinanden. Summen af søgte oplysninger svarer til summen af de forskellige resultater, som efterforskningstjenesterne afhængigt af deres adgangstilladelser opnår fra de forskellige databaser.

2.7. Kommissionen søger at svare på følgende spørgsmål:

— med hvilken metode kan man uden at ændre på de allerede etablerede systemer, og uden at komplementariteten går tabt, få alle databaser afstemt med hinanden på samme tid, så man ved et indrejsested til europæisk område med én enkelt søgning i systemet kan sikre, at alle allerede indsamlede oplysninger i de eksisterende databaser fremsendes til den tilsynsmyndighed, der har beføjelser til at samkøre dem under overholdelse af bestemmelserne om databeskyttelse og beskyttelse af de grundlæggende rettigheder?

2.8. Med de fremsatte forslag ønsker Kommissionen:

2.8.1. at udvide mulighederne ved adgang til databaserne hos Europol og Interpol, som allerede samarbejder med de europæiske tilsynsmyndigheder;

2.8.2. at »synkronisere« informationssøgningerne for at reducere svartiderne i forbindelse med behandlingen af migranters sager og accelerere den sikkerhedsmæssige reaktion, når dette er nødvendigt. Med henblik herpå foreslår den, at der oprettes nye enheder, som gør det muligt for de nuværende databaser at tale med hinanden.

2.9. **Målene er så vidt muligt at afhjælpe manglerne ved de enkelte systemer, forbedre** forvaltningen af Schengenområdets ydre grænser, bidrage til EU's interne sikkerhed, håndtere identitetstyveri, løse sager om anvendelse af flere identiteter, finde personer, der er under mistanke eller allerede er dømt, og kontrollere deres identitet i Schengenområdet.

2.10. For at vende tilbage til sammenligningen med en smartphone vil den ansvarlige myndighed ikke alene have adgang til adskillige apps, men vil også samtidig og inden for rammerne af den samme søgning ved hjælp af adgangskoder kunne indsamle data, der er lagret på alle medier, PC'er, laptops, telefoner, tablets, notebooks osv.

([2]) EUT C 34 af 2.2.2017, s. 144.
([3]) EUT C 458 af 19.12.2014, s. 36.
([4]) EUT C 487 af 28.12.2016, s. 66.
([5]) EUT C 246 af 28.7.2017, s. 28.

3. **Systemets funktionsmåde**

3.1. Kommissionen har afholdt høringer og nedsat en ekspertgruppe på højt niveau ([6]) vedrørende informationssystemer og interoperabilitet, hvis medlemmer udpeges af medlemsstaterne, landene i Schengengruppen, europæiske agenturer som eu-LISA2 ([7]) og Agenturet for Grundlæggende Rettigheder ([8]), og som koordineres af GD HOME.

Metode: sammenkobling eller interoperabilitet?

3.1.1. **Sammenkobling** af informationssystemer giver mulighed for at forbinde dem indbyrdes, således at data fra ét system automatisk kan hentes fra et andet system.

3.1.2. **Interoperabilitet** ([9]) er forskellige systemers kapacitet til at kommunikere, udveksle data og anvende de udvekslede oplysninger under overholdelse af adgangsrettighederne til systemerne.

3.2. *Valg af interoperabilitet*

3.2.1. Kommissionen mener ikke, at denne option vil medføre grundlæggende ændringer af de nuværende systemer og kompetencer, og dataene vil fortsat være adskilt fra hinanden. Trods de øgede kommunikationsmuligheder vil det betyde øget sikkerhed af systemer og data, der naturligvis ikke vil være tilgængelige via internettet. De kommissionsforslag, som er genstand for denne udtalelse, indeholder mange lighedspunkter og vedrører:

— for det ene forslags vedkommende (COM(2017) 793 final) interoperabilitet mellem informationssystemer for grænser og visa,

— for det andet forslags vedkommende (COM(2017) 794 final) politisamarbejde og samarbejde om retlige anliggender samt asyl og migration.

3.3. *De nye værktøjer*

3.3.1. For at interoperabiliteten skal kunne fungere, skal en ny struktur bestående af fire nye værktøjer supplere de seks databaser med det formål at accelerere arbejdet, idet man kun behøver at foretage én søgning. Det skal dog til enhver tid sikres, at der står et menneske bag søgningerne.

3.4. *ESP, en europæisk søgeportal*

3.4.1. Den ansvarlige tilsynsmyndighed (slutbrugeren) bør have adgang til hele systemet fra ét og samme sted. I stedet for at foretage seks søgninger kan man via én enkelt forespørgsel (politi, toldvæsen osv.) søge efter de ønskede oplysninger i flere databaser samtidig uden selv at lagre oplysninger. Hvis oplysningerne findes, finder systemet dem. I tilfælde af mistanke om kriminalitet eller terrorvirksomhed giver den første søgning måske et neutralt resultat for den kontrollerede person (»no-hit«), men hvis dette resultat matcher med en anden oplysning (»hit«), der kan findes i databaser som SIS, EES eller ETIAS, kan det føre til mere dybtgående søgninger og en undersøgelse.

3.5. *Fælles BMS (det fælles biometrisystem)*

3.5.1. Denne fælles matching-platform gør det muligt at søge i og samtidig foretage sammenligninger af matematiske og biometriske data, digitale fingeraftryk og pasbilleder fra forskellige databaser som SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, men ikke fra *ETIAS*; dataene i disse databaser skal være kompatible.

3.5.2. De matematiske data lagres ikke i deres oprindelige form.

3.6. *CIR (det fælles identitetsregister)*

3.6.1. Det »fælles identitetsregister« indsamler data om den biografiske og biometriske identitet af tredjelandsstatsborgere, der er blevet kontrolleret enten ved grænserne eller i medlemsstaterne (Schengenområdet). En indikator for match mellem oplysningerne i de forskellige databaser gør søgningerne hurtigere. Ansvaret for dataene ligger hos eu-LISA, som via sine sikkerhedsforanstaltninger lagrer dem, således at ingen kan få adgang til mere end én alfanumerisk linje ad gangen. CIR er udviklet på grundlag af EES og ETIAS og burde ikke føre til en duplikering af dataene. Registeret vil også kunne anvendes til søgninger til civile formål.

([6]) GD HOME, kontor B/3; Kommissionens afgørelse C/2016/3780 af 17. juni 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=DA

([7]) Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed.

([8]) EU's Agentur for Grundlæggende Rettigheder.

([9]) Kommissionens meddelelse, COM(2016) 205 final, Stærkere og mere intelligente informationssystemer for grænser og sikkerhed.

([10]) Kursiveringen angiver, at retsakterne vedrørende disse organer endnu ikke er blevet vedtaget.

3.7. *MID (multiidentitetsdetektoren)*

3.7.1. Detektorens rolle består i at sikre en korrekt identificering af personer i god tro og bekæmpe identitetstyveri gennem en parallel søgning i alle databaser. Ingen myndigheder har endnu anvendt et lignende værktøj, der skal gøre det muligt at undgå identitetstyveri.

3.8. *eu-LISA-agenturets rolle* ([11])

3.8.1. Agenturet blev oprettet i 2011 og har til opgave at fremme gennemførelsen af EU's politikker inden for området retfærdighed, sikkerhed og frihed. Det er baseret i Tallinn (Estland) og sørger allerede for, at der kan udveksles oplysninger mellem de forskellige retshåndhævende myndigheder i medlemsstaterne, at store IT-systemer kan fungere uhindret, og at personer kan bevæge sig frit i Schengenområdet.

3.8.2. Det arbejder på projektet »Smart Borders« og dets rolle i den nye struktur for dataudveksling består i at opbevare oplysninger om personer og myndigheder, undersøgelser og undersøgelsestjenester. Agenturet fører tilsyn med de oplysningssøgendes adgangsrettigheder og er ansvarligt for datasikkerheden, herunder i tilfælde af »sikkerhedshændelser« (artikel 44, COM(2017) 793 og 794 final).

3.8.3. Med **UMF** (det universelle meddelelsesformat), som endnu ikke er færdigudviklet, bliver det nemmere at arbejde med de nye systemer, hvis anvendelse bliver obligatorisk og vil kræve, at der udvikles grænseflader i de medlemsstater, der endnu ikke har sådanne, og et system for midlertidig oversættelse fra et sprog til et andet.

3.9. *Beskyttelse af personoplysninger (artikel 8 og 7 i chartret):*

3.9.1. I forslaget til forordning erkendes det, at der kan opstå sikkerhedshændelser. Medlemsstaterne og deres datasystemer skal i første række overholde principperne om databeskyttelse som nedfældet i kommissionsforslagene, traktaten, chartret om grundlæggende rettigheder og den generelle forordning om databeskyttelse ([12]), der træder i kraft den 25. maj 2018.

4. **Diskussion**

4.1. *Merværdien af interoperabilitet i et demokrati*

4.1.1. EU har brug for regulering og undersøgelsesmekanismer, der beskytter Unionen mod kriminalitet. Interoperabilitet mellem informationssystemerne gør det muligt at håndhæve retsstatsprincippet og beskytte menneskerettighederne.

4.1.2. *EES og ETIAS* vil — når de sammenkobles med BMS og CIR — gøre det muligt at kontrollere grænsepassager, som foretages af mistænkte, og at lagre oplysninger om dem. De retshåndhævende myndigheders mulighed for (via BMS) at få »adgang til informationssystemer, som ikke vedrører retshåndhævelse, på EU-niveau« (artikel 17 i forslaget til forordning vedrørende CIR, COM(2017) 794 og 793 final) er ikke forenelig med de målsætninger, som ligger til grund for de behandlede forslag. EØSU (artikel 300, stk. 4, i TEUF) må i den sammenhæng henvise til proportionalitetsprincippet og anmode Kommissionen om at undgå enhver big brother-lignende ordning ([13]), der skaber hindringer for europæernes frie bevægelighed (artikel 3 i TEU).

4.1.3. Den foreslåede model for indsamling og anvendelse af personoplysninger, der indhentes ved grænserne og inden for Unionen i forbindelse med kontrol af personers rejseruter og dokumenter, fremstilles som værende et vandtæt system, der kun er tilgængeligt for bemyndigede personer til sikkerhedsrelaterede og grænseforvaltningsmæssige formål. Det vil gøre procedurerne mere gnidningsfrie.

4.1.4. EØSU sætter spørgsmålstegn ved, hvor vandtæt systemet er, for der vil fortsat være mangler, og systemets gradvise indførelse over en niårig periode skal understøttes af »fundamenter«, der endnu ikke eksisterer, såsom EES- og ETIAS-databaserne samt nationale grænseflader. Teknologien er i konstant udvikling, og projektet må nødvendigvis baseres på den nuværende teknologi, og der er ikke afsat budgetmidler til håndtering af den teknologiske forældelse, der vil opstå inden for visse digitale sektorer.

([11]) Europa-Parlamentets og Rådets forordning (EU) nr. 1077/2011 af 25. oktober 2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store it-systemer inden for området med frihed, sikkerhed og retfærdighed.

([12]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse). EØSU-udtalelser: EUT C 229 af 31.7.2012, s. 90 og EUT C 345 af 13.10.2017, s. 138.

([13]) I »1984«, George Orwell.

4.1.5. Desuden kunne man have medtaget den hurtige vækst i brugen af algoritmer med såkaldt kunstig intelligens i projektet både som kontrolværktøj for systemerne og som en sikkerhedsnøgle, der kan overdrages til de beslutningstagende myndigheder som led i sikringen af en demokratisk anvendelse af strukturen.

4.1.6. I forslaget udvikles der et system for lovlydige personer, der handler i god tro. Det er betryggende, at det er mennesker, der sidder ved roret, men de kan også udgøre det svage led. EØSU foreslår, at man tilføjer en artikel om »mekanismer til afbrydelse af systemet« til brug i forbindelse med politiske kriser og/eller forvaltningsproblemer, idet alle problemer i en database kan udgøre en risiko for hele strukturen ([14]). En generel udbredelse af UMF kunne føre til en international anvendelse, hvilket ville få en meget positiv effekt på, men også udgøre en risiko for beskyttelsen af data. De ansvarlige myndigheder ville komme til at bære et tungt ansvar. Disse aspekter er ikke medtaget i de behandlede kommissionsforslag.

4.2. *Beskyttelse af de grundlæggende rettigheder*

4.2.1. De grundlæggende rettigheder er absolutte og kan kun begrænses, hvis dette er nødvendigt og faktisk svarer til mål af almen interesse, der er anerkendt af EU, og hvis deres væsentligste indhold respekteres (artikel 8 og 52, stk. 1, i chartret om grundlæggende rettigheder). EØSU undrer sig over, hvordan man kan vurdere proportionaliteten af kontrolforanstaltninger, når der er tale om migranter, der flygter fra forfølgelse og ankommer til EU's kyster. (COM(2017) 794 final, Begrundelse — grundlæggende rettigheder). Eftersøgningen af mistænkte med henblik på at forebygge kriminelle handlinger, navnlig terror, må ikke føre til, at **vore demokratier udvikler sig til samfund, hvor man straffes for handlinger, som man endnu ikke har begået**. Man bør sondre mellem »handlinger«, der forstyrrer den offentlige orden, og »holdninger«.

4.2.2. Overholdelsen af de i chartret formulerede rettigheder for alle personer skal sikre en balance mellem sikkerhed og frihed, da demokratiet uden denne balance ikke vil kunne overleve. EØSU mener, at en sådan balance er af afgørende betydning og bør være et permanent mål for alle myndigheder, herunder tilsynsmyndighederne, på såvel nationalt som europæisk plan.

4.2.3. Oplysninger om, hvilke myndigheder der medvirker ved undersøgelser, og de tilhørende metadata vil blive lagret i systemet. De ansvarlige myndigheders egne grundlæggende rettigheder skal ligeledes overholdes i forbindelse med genereringen af data, navnlig med hensyn til deres sikkerhed og privatliv, i tilfælde af ondsindet indtrængen i strukturen og misbrug af data mellem indsamlings- og sletningstidspunktet.

4.3. *Databeskyttelse*

4.3.1. I Kommissionens forslag anerkendes princippet om beskyttelse af personoplysninger gennem design og standardindstillinger, selv om der i begrundelsen mindes om, at der ifølge EU-Domstolen ikke er tale om en absolut rettighed. EØSU anerkender fordelene ved at træffe forebyggende foranstaltninger, der skal garantere sikkerheden, bekæmpe falske identiteter og sikre retten til asyl. Men udvalget ønsker at understrege begrænsningerne ved matematisering og anonymisering af data, idet de berørte personer på et senere tidspunkt kan få brug for deres data.

4.3.2. EØSU understreger ligeledes, at typen af de data, som lagres — biometriske og biologiske — er af særlig interesse for visse virksomheder og i forbindelse med kriminalitet. Cybersikkerhed er i den sammenhæng lige så vigtig som fysisk sikkerhed og omtales ikke i tilstrækkelig grad i kommissionsforslagene. Dataene lagres på ét enkelt fysisk sted, der — selv om det er sikret — kan blive hacket.

4.3.3. EØSU minder om, at EU's institutioner og organer, for så vidt angår databeskyttelse og retten til at få slettet data (retten til at blive glemt), er underlagt forordning (EF) nr. 45/2001, som yder mindre beskyttelse end den generelle forordning om databeskyttelse ([15]) fra 2016 (der træder i kraft i maj 2018), som medlemsstaterne skal overholde. Udvalget understreger kompleksiteten ved håndhævelsen af denne ret og tvivler på, at rejsende, migranter og asylansøgere er i stand til at påberåbe sig den:

1) Beskyttelsen af personoplysninger skal godkendes for alle eksisterende databaser, både nationale og europæiske, for således at sikre, at samtlige data er beskyttede.

2) Denne beskyttelse er en forudsætning for, at borgerne accepterer dette enorme overvågningsnet.

4.3.4. Det præciseres ikke klart i kommissionsforslagene, i hvor lang tid de ansvarlige myndigheder opbevarer de indsamlede data. I forslagene omtales proceduren for udøvelse af retten til at få berigtiget og/eller slettet data, der foregår mellem den stat, hvortil anmodningen er rettet, og den stat, der er ansvarlig for behandlingen heraf. Der fastsættes dog ikke nogen tidsfrist for opbevaringen af dataene (artikel 47 i kommissionsforslagene). EØSU anbefaler, at der fastsættes en tidsfrist, og at denne bliver kortere for mindreårige (artikel 24 i chartret), medmindre der er tale om terrorsager, så disse får bedre mulighed for at integrere sig.

([14]) Den Europæiske Tilsynsførende for Databeskyttelse, den endelige rapport fra ekspertgruppen på højt niveau, maj 2017.
([15]) Den generelle forordning om databeskyttelse [forordning (EU) 2016/679].

4.4. *Forvaltning og sikring af ansvarlighed*

4.4.1. Internationale databaser er ikke underlagt de samme regler som europæiske IT-systemer. Indførelsen af et universelt adgangsformat, der med tiden kan få international udbredelse, ville blot være et teknisk aspekt, der ikke samordner bestemmelserne, selv om Interpol naturligvis skal overholde artikel 17 i FN's konvention ([16]). Godkendelserne vil i øvrigt stadig henhøre under medlemsstaternes kompetence. EØSU mener, at dette spørgsmål bør tages op i forslagene.

4.4.2. Én enkelt søgning vil være nok til at opnå samtlige ønskede oplysninger fra de europæiske databaser. EØSU understreger, at det heraf følgende bureaukrati i høj grad opvejes af den tid, man vinder. Forvaltningen forestås af Kommissionen og medlemsstaterne inden for rammerne af en kontrolprocedure. eu-LISA bliver omdrejningspunktet og har navnlig til opgave at sikre, at der er indført procedurer for indsamlingen af oplysninger om, hvordan interoperabilitetskomponenterne fungerer. Agenturet modtager oplysninger fra medlemsstaterne og Europol og forelægger hvert fjerde år en teknisk evalueringsrapport for Rådet, Europa-Parlamentet og Kommissionen, mens Kommissionen selv udarbejder en samlet rapport et år efter (artikel 68 i kommissionsforslagene). EØSU mener, at disse tidsrammer er for lange. Vurderingen af sikkerheden ved interoperabilitetskomponenterne (artikel 68, stk. 5, litra d)) bør som et minimum foretages hvert år, og evalueringen af indvirkningen på de grundlæggende rettigheder bør som et minimum foretages hvert andet år (artikel 68, stk. 5, litra b)).

4.4.3. EØSU beklager, at så grundlæggende spørgsmål som dem, der tages op i forslagene, skal håndteres af EU-agenturer, hvis rekrutteringsprocedurer og opgaver er uklare for mange borgere. EØSU finder det nødvendigt at udveksle god praksis og høre alle uafhængige tilsynsmyndigheder med ansvar for kontrol med anvendelsen af data (Den Europæiske Tilsynsførende for Databeskyttelse) og andre agenturer, herunder Agenturet for Grundlæggende Rettigheder og ENISA.

4.4.4. Alle disse nye strukturer og procedurer skal indføres via Kommissionens delegerede retsakter og gennemførelsesretsakter. EØSU ser gerne, at målsætningen om overholdelse af de grundlæggende rettigheder og beskyttelse af personoplysninger forbliver forankret i alle disse retsakter med henblik på at sikre en bedre modtagelse af personer ved grænserne. Udvalget anbefaler, at de europæiske borgere frem til afslutningen af projektet holdes orienteret om projektets enkelte etaper, og at de berørte personer på en letforståelig måde informeres om den kontrol, som de er underlagt.

5. **De europæiske tilsynsmyndigheders uddannelsesbehov**

5.1. EØSU mener, at der vil være et stort behov for uddannelse i den første periode (efter 2021), i modsætning til hvad Kommissionen giver udtryk for i sin konsekvensanalyse (C). Den taler om 76 mio. EUR om året. Overgangen til nye procedurer kræver altid en opdatering. Dette gælder for alle EU's grænser og alle nationale systemer. Nogle medlemsstater har endnu ikke kompatible systemer og skal yde en stor indsats for at udvikle grænseflader, der sætter dem i stand til at deltage. For at interoperabiliteten skal fungere, bør forskellene mellem medlemsstaterne udviskes.

5.2. Uddannelse i korrekt anvendelse af kvalitetsdata og UMF vil få stor betydning. EØSU foreslår, at der i samarbejde med bl.a. Cepol ([17]), Frontex og Europol tilrettelægges fælles uddannelser for de ansvarlige myndigheder, herunder eu-LISA, hvis medlemmer skal have deres kompetencer set efter i sømmene.

5.3. Et værktøj som MID findes ingen andre steder. Hvis det bliver vellykket, vil det få stor gennemslagskraft. Den nye struktur forudsætter data af den bedst mulige kvalitet. Hvis hele systemet skal leve op til forventningerne til projektet, skal alle medlemsstater deltage på samme niveau, da manglerne ellers vil blive alvorligere end tidligere, hvilket vil udhule retten til asyl og international beskyttelse (artikel 18 og 19 i chartret).

6. **Finansiering.**

6.1. Hele den foreslåede struktur bygger på en række antagelser: at de ansvarlige myndigheder indfører *EES, ETIAS* og *UMF*-systemerne, at *MID* fungerer korrekt, og at *CIR* er sikkert. Spørgsmålet er, om de to organer, Den Europæiske Tilsynsførende for Databeskyttelse og eu–LISA, og måske også ENISA, råder over tilstrækkelige menneskelige og økonomiske ressourcer. Kommissionen anbefaler medfinansiering mellem EU og medlemsstaterne. EØSU bemærker, at forvaltningen af det europæiske semester stadig finansieres gennem stramme budgetter, og at den nuværende anvendelse af de eksisterende databaser (SIS, VIS, Prüm og *EES*) stadig skal optimeres under overholdelse af de juridiske krav (rapport fra ekspertgruppen).

([16]) Den internationale konvention om borgerlige og politiske rettigheder, FN: Artikel 17, stk. 1, — »Ingen må udsættes for vilkårlig eller ulovlig indblanding i sit privatliv eller familieliv, sit hjem eller sin brevveksling, eller for ulovlige angreb på sin ære og sit omdømme. Stk. 2. Enhver har ret til lovens beskyttelse mod sådan indblanding eller sådanne angreb.«

([17]) Cepol, Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Budapest, Ungarn).

6.2. EØSU vil gerne vide, hvilke budgetmæssige konsekvenser Brexit kommer til at få, selv om Det Forenede Kongerige ikke er med i Schengensystemet, og mere generelt, hvorvidt den fremtidige forvaltning af interoperabiliteten vil være kompleks i europæiske lande, som ikke er med i SIS, men som deltager i andre systemer såsom Eurodac.

6.3. Den fond, der efter planen skal anvendes, er Fonden for Intern Sikkerhed. Den ventes at blive taget i brug i 2023. EØSU er i tvivl om, hvorvidt fem år er tilstrækkeligt til at mindske forskellene mellem de europæiske lande og skabe betingelserne for succes. Det planlagte budget er på 424,7 mio. EUR over ni år (2019-2027). EU (dvs. Fonden for Intern Sikkerhed) og medlemsstaterne skal betale. Medlemsstaterne skal sikre, at de er i stand til at få de nuværende systemer til at fungere korrekt sammen med den nye IT-struktur. EØSU vurderer, at fornyet vækst vil kunne bidrage til gennemførelsen af disse investeringer.

Bruxelles den, 23. maj 2018.

Luca JAHIER
Formand
for Det Europæiske Økonomiske og Sociale Udvalg