Advies van het Europees Economisch en Sociaal Comité over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van een kader voor interoperabiliteit tussen de EU-informatiesystemen (grenzen en visa) en tot wijziging van Beschikking 2004/512/EG van de Raad, Verordening (EG) nr. 767/2008, Besluit 2008/633/JBZ van de Raad, Verordening (EU) 2016/399 en Verordening (EU) 2017/2226

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

en het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van een kader voor interoperabiliteit tussen de EU-informatiesystemen (politiële en justitiële samenwerking, asiel en migratie)

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

(2018/C 283/07)

Rapporteur: **Laure BATUT**

Raadpleging	Europese Commissie, 18.1.2018
	Europees Parlement: 28.2.2018
Rechtsgrondslag	Artikel 304 van het Verdrag betreffende de werking van de Europese Unie
Bevoegd	Afdeling Werkgelegenheid, Sociale Zaken en Burgerschap
Goedkeuring door de afdeling	25.4.2018
Goedkeuring door de voltallige vergadering	23.5.2018
Zitting nr.	535
Stemuitslag	160/3/2
(voor/tegen/onthoudingen)	

1. **Conclusies en aanbevelingen**

1.1. Het Europees Economisch en Sociaal Comité (EESC) is ingenomen met het voorstel van de Europese Commissie om de interoperabiliteit van de grens- en visuminformatiesystemen van de EU en de samenwerking op het gebied van politie, justitie, asiel en migratie te verbeteren.

1.2. Het EESC is van mening dat interoperabiliteit een strategische doelstelling van de EU moet zijn, wil zij een open ruimte blijven die de grondrechten en mobiliteit waarborgt. De EU en de lidstaten zijn verplicht het leven en de veiligheid van alle mensen te beschermen; het beginsel van non-refoulement moet ten volle in acht worden genomen.

1.3. Interoperabiliteitsmaatregelen zullen beter worden begrepen als ze

— in het kader van de EU-migratiestrategie de voorwaarden garanderen voor een evenwicht tussen vrijheid en veiligheid, met inachtneming van de scheiding der machten;

— de grondrechten van de betrokken personen garanderen, met name de beveiliging van hun persoonsgegevens en hun privéleven, het recht op toegang tot, alsook rechtzetting en verwijdering van hun gegevens binnen een redelijke termijn, via toegankelijke procedures;

— ervoor zorgen dat ook in alle uitvoeringsbepalingen wordt bevestigd dat vanaf de ontwerpfase rekening moet worden gehouden met de beginselen van gegevensbescherming („privacy by design”);

— geen nieuwe belemmeringen voor het normale verkeer van personen en goederen in het leven roepen.

1.4. Het EESC dringt aan op procedures en garanties voor het gebruik van gegevens voor rechtshandhavingsdoeleinden die:

— voorzien in toepassing van de Europese wetgeving die de meeste bescherming biedt (algemene verordening gegevensbescherming);

— de besluitvorming kunnen versnellen in de lidstaat die de verzoeken om internationale bescherming moet behandelen;

— de betrokkenen het recht op rechtspraak in dubbele aanleg garanderen;

— minderjarigen en in het bijzonder niet-begeleide minderjarigen, ongeacht of zij zich in een irreguliere situatie bevinden, vervolgd worden of een misdrijf hebben gepleegd, het recht garanderen om te veranderen, een visum te krijgen, beschermd en geïntegreerd te worden alsook te worden vergeten binnen een kortere termijn dan voor meerderjarigen geldt.

1.5. Het EESC is van mening dat de huidige rechtsgrondslag voor informatiesystemen moet worden versterkt en dat daarbij rekening moet worden gehouden met de ontwikkeling van gegevensverzamelingssystemen. Het pleit voor:

— versterking van de veiligheid van bestaande databanken en hun communicatiekanalen;

— een evaluatie van de impact van de versterkte controle vooraf op het risicobeheer;

— een permanente controle en evaluatie van het systeem door de autoriteiten voor gegevensbescherming (EDPS); van de verantwoordelijke personen eist het dat zij jaarlijks verslag doen aan de beslissingsautoriteiten en de Commissie over de beveiliging van de interoperabiliteitsonderdelen, alsook tweejaarlijks over de gevolgen van de maatregelen voor de grondrechten.

1.6. Het EESC is van mening dat het project moet worden ondersteund door deskundig personeel en dringt aan op

— degelijke opleidingsprogramma's voor de betrokken overheden en het personeel van eu-LISA;

— een strikte controle van de vaardigheden van het personeel en de kandidaten voor functies bij dit agentschap.

1.7. Het EESC maakt zich zorgen over de financiering van het nieuwe systeem. Het toezicht op de planning zal van cruciaal belang zijn om ontsporing van de begroting te voorkomen en het project in 2029 tot een goed einde te brengen.

1.8. Het EESC zou graag zien dat de burgers worden geïnformeerd over de voortgang van het project tot de voltooiing ervan, en dat zij educatieve informatie krijgen over de controles die zij moeten ondergaan. Het is van mening dat moet worden voorzien in de mogelijkheid om alles stop te zetten als de vrijheid en de grondrechten worden bedreigd door misbruik van het systeem.

2. **Inleiding**

2.1. In het licht van de internationale toestand in 2017 die, zowel op geopolitiek gebied als ten aanzien van de binnenlandse veiligheid van de lidstaten, als onstabiel wordt beschouwd heeft de Raad de Commissie herhaaldelijk verzocht ervoor te zorgen dat personen die als „risicovol" worden beschouwd en van wie reeds in een van de lidstaten een signalement bestaat kunnen worden opgespoord. Voor de veiligheid in de EU kan het van wezenlijk belang zijn na te gaan waar en wanneer ze de grens zijn overgestoken en welke reizen en trajecten ze hebben afgelegd.

2.2. In zijn resolutie van 6 juli 2016 heeft het Europees Parlement de Commissie verzocht te voorzien in de nodige garanties wat betreft gegevensbescherming.

2.3. De voorliggende teksten sluiten aan bij de doelstelling „Instandhouding en versterking van Schengen" ([1]). De EU beschikt reeds over verschillende regelingen en digitale informatiediensten op gebieden die verband houden met grenscontroles van personen en goederen.

2.4. Ter herinnering:

— **SIS: het Schengeninformatiesysteem**, een van de oudste systemen, dat is herzien en een breed spectrum van waarschuwingen over personen en goederen beheert;

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

— **Eurodac: het Europese systeem voor de vergelijking van vingerafdrukken** van asielzoekers en irreguliere onderdanen van derde landen aan de buitengrenzen en binnen de lidstaten, en voor de vaststelling van de lidstaat die verantwoordelijk is voor de behandeling van de verzoeken (CESE 2016-02981, rapporteur: Moreno Díaz ([2]));

— **VIS: het visuminformatiesysteem** (visumcode) voor het beheer van visa voor verblijven van korte duur (CESE 2014-02932, rapporteurs: Pezzini en Pariza Castaños ([3]));

— **EES: het inreis-uitreissysteem**, waarover thans nog een besluit moet worden genomen en dat bedoeld is voor het elektronische beheer van paspoortgegevens en inreis-uitreisdata van onderdanen van derde landen die het Schengengebied bezoeken (CESE 2016-03098 SOC/544, rapporteur: Pîrvulescu ([4]));

— **ETIAS: het Europees systeem voor reisinformatie en -autorisatie** waarover thans nog een besluit moet worden genomen en dat bedoeld is als een groot geautomatiseerd systeem voor opslag en controle vooraf van gegevens van onderdanen van derde landen die vrijgesteld zijn van visumplicht om in het Schengengebied te reizen (CESE 2016-06889 SOC/556, rapporteur: Simons ([5]));

— **ECRIS-TCN: het Europees systeem voor de uitwisseling van informatie over strafregisters van onderdanen van derde landen**, dat thans wordt voorgesteld door de Commissie, een digitaal systeem voor de uitwisseling van informatie over reeds door nationale rechtbanken genomen rechterlijke beslissingen.

2.5. De middelen waarover een bevoegde overheid thans beschikt, kunnen worden voorgesteld als een smartphone met verschillende toepassingen die allemaal van elkaar gescheiden zijn en hun „eigen" informatie verstrekken.

2.6. Met uitzondering van het SIS zijn deze systemen gericht op het **beheer van onderdanen van derde landen**. Er zijn zes elkaar aanvullende gedecentraliseerde systemen. De som van de gezochte informatie zijn de verschillende antwoorden die uit de verschillende databanken zijn verkregen door de opsporingsdiensten, afhankelijk van hun toegangsrechten.

2.7. De Commissie wil de volgende vraag beantwoorden:

— met welke methode, zonder te raken aan de bestaande structuren en met behoud van hun complementariteit, kunnen alle databanken op elkaar worden afgestemd, zodat op de plek van binnenkomst op het Europese grondgebied en door één bevraging van het systeem alle inlichtingen die reeds in bestaande databanken zijn opgeslagen samenkomen bij de controleautoriteit die bevoegd is ze te bevragen, met inachtneming van de regels inzake gegevensbescherming en grondrechten?

2.8. In de voorliggende voorstellen zou de Europese Commissie graag zien dat:

2.8.1. wordt voorzien in extra mogelijkheden van toegang tot de databanken van Europol en Interpol, die reeds met de Europese toezichthoudende autoriteiten samenwerken;

2.8.2. het informatieonderzoek wordt „gesynchroniseerd" om de responstijd m.b.t. het dossier van migranten te verkorten, en indien nodig sneller werk te maken van een beveiligingsreactie. Met het oog daarop wil zij nieuwe entiteiten in het leven roepen, die de bestaande structuren nauwer zouden laten samenwerken.

2.9. **Doel is de lacunes van de verschillende systemen zo veel mogelijk aan te vullen**; het beheer van de buitengrenzen van het Schengengebied te verbeteren; bij te dragen aan de interne veiligheid van de Unie; identiteitsfraude aan te pakken; gevallen van meervoudige identiteit op te lossen; verdachte of reeds veroordeelde personen op te sporen en hun identiteit in het Schengengebied te verifiëren.

2.10. Om terug te grijpen naar het beeld van de smartphone: de bevoegde autoriteit zou niet alleen tal van toepassingen ter beschikking hebben maar zou ook tegelijkertijd en in het kader van eenzelfde onderzoek, met behulp van toegangscodes, de gegevens kunnen opvragen die opgeslagen zijn op alle dragers: PC, laptop, telefoon, tablet, notebook enz.

([2]) PB C 34 van 2.2.2017, blz. 144.
([3]) PB C 458 van 19.12.2014, blz. 36.
([4]) PB C 487 van 28.12.2016, blz. 66.
([5]) PB C 246 van 28.7.2017, blz. 28.

3. **Werking van het systeem**

3.1. De Europese Commissie heeft raadplegingen gehouden en een door DG HOME gecoördineerde groep op hoog niveau opgericht met deskundigen inzake informatiesystemen en interoperabiliteit ([6]) die zijn benoemd door de lidstaten, de landen van de Schengengroep, Europese agentschappen zoals eu-LISA ([7]) en FRA ([8]).

De methode: interconnectiviteit of interoperabiliteit?

3.1.1. **Interconnectiviteit** van informatiesystemen betreft de mogelijkheid om systemen zo aan elkaar te koppelen dat de gegevens van het ene systeem automatisch toegankelijk zijn voor het andere.

3.1.2. **Interoperabiliteit** ([9]) is het vermogen van verschillende systemen om te communiceren, onderling gegevens uit te wisselen en de uitgewisselde informatie te gebruiken, met inachtneming van de systeemtoegangsmachtigingen.

3.2. *De keuze voor interoperabiliteit*

3.2.1. De Commissie is van mening dat de verworvenheden van de huidige structuren en bevoegdheden hierdoor niet in het gedrang komen en dat de gegevens „gecompartimenteerd" zullen blijven. Hoewel aldus gemakkelijker gecommuniceerd zal kunnen worden, zal dit toch de veiligheid ten goede komen van de systemen en de gegevens die uiteraard niet toegankelijk zullen zijn via internet. De voor advies voorgelegde teksten zijn zeer vergelijkbaar maar betreffen

— enerzijds (COM(2017) 793) de interoperabiliteit van grens- en visuminformatiesystemen,

— anderzijds (COM(2017) 794) politiële en justitiële samenwerking, asiel en migratie.

3.3. *De nieuwe instrumenten*

3.3.1. Om interoperabel te kunnen werken moeten de zes basissystemen worden aangevuld met een nieuw systeem van vier nieuwe instrumenten die, om snel te werken, het systeem maar één keer zullen bevragen, met steeds bevoegde personen aan de oorsprong van de bevragingen.

3.4. *Het ESP, het Europees zoekportaal*

3.4.1. De bevoegde toezichthoudende autoriteit (de eindgebruiker) moet beschikken over een unieke toegang tot het hele systeem. In plaats van zes zoekopdrachten zal er nog maar één worden gelanceerd (door politie, douane enz.) waarbij verschillende databanken gelijktijdig op de gevraagde gegevens zullen worden doorzocht zonder evenwel enige gegevens op te slaan. Als de gegevens bestaan, zal het systeem ze vinden. Ingeval een misdaad of een terroristische activiteit wordt vermoed kan de eerste hit voor de gecontroleerde persoon neutraal uitpakken („no-hit"), maar wanneer de informatie overeenstemt met een tweede gegeven („hit") in bestaande databanken als SIS, EES, ETIAS, dan kan dit leiden tot grondiger onderzoek en een enquête.

3.5. *Het gezamenlijk BMS (Shared Biometric Matching Service — Gemeenschappelijke dienst voor biometrische matching)*

3.5.1. Dit gemeenschappelijk matchingplatform zal het mogelijk maken mathematische en biometrische gegevens, vingerafdrukken en identiteitsfoto's tegelijkertijd op te zoeken in verschillende databanken zoals SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, maar niet *ETIAS*, en ze te vergelijken; de betreffende gegevens moeten compatibel zijn.

3.5.2. De mathematische gegevens zullen niet in hun oorspronkelijke vorm worden bewaard.

3.6. *Het CIR (Common Identity Repository — Gemeenschappelijk identiteitsregister)*

3.6.1. In het „gemeenschappelijk register van identiteitsgegevens" zullen de gegevens over de biografische en biometrische identiteit worden opgeslagen van onderdanen van derde landen die aan de grens of in de (Schengen)lidstaten worden gecontroleerd. Een indicator voor treffermarkering in de verschillende databanken zal het zoekwerk versnellen. Onder de verantwoordelijkheid en met de beveiligingsmiddelen van het eu-LISA-agentschap zullen deze gegevens zo worden opgeslagen dat niemand meer dan één alfanumerieke lijn tegelijk kan openen. Het op basis van EES en ETIAS ontwikkelde CIR mag niet tot duplicatie van gegevens leiden. Het register zal ook kunnen worden gebruikt voor civiel onderzoek.

([6]) DG HOME, eenheid B/3; Besluit C/2016/3780 van de Commissie van 17 juni 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=NLhttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=NL

([7]) Europees Agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

([8]) FRA: Bureau van de Europese Unie voor de grondrechten.

([9]) Commissiemededeling, COM(2016) 205 final, „Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid".

([10]) De teksten met betrekking tot de cursief vermelde organen zijn nog niet goedgekeurd.

3.7. *De MID (Multiple-Identity Detector — detector van meerdere identiteiten)*

3.7.1. Hiermee zal de juiste identiteit van bonafide personen kunnen worden gecontroleerd en zal identiteitsfraude kunnen worden bestreden door alle databanken tegelijkertijd te doorzoeken. Dit instrument is nog door geen enkele administratie gebruikt en moet misbruik van identiteit helpen voorkomen.

3.8. *Rol van het eu-LISA-agentschap* ([11])

3.8.1. Het in 2011 opgerichte agentschap heeft tot taak het EU-beleid op het gebied van vrijheid, veiligheid en recht te vergemakkelijken. Het is gevestigd te Tallinn in Estland en zorgt thans reeds voor uitwisseling van informatie tussen de verschillende rechtshandhavingsautoriteiten van de lidstaten, de naadloze werking van grootschalige informaticasystemen en het vrije verkeer van personen in het Schengengebied.

3.8.2. Het agentschap werkt aan het project „Smart Borders" en zal in de nieuwe structuur voor gegevensuitwisseling een rol spelen in de bewaring van persoonsgebonden gegevens zoals gegevens i.v.m. autoriteiten, onderzoeken en onderzoekers. Het zal de vergunningen van de aanvragers controleren en de gegevensbeveiliging waarborgen, ook in geval van „incidenten" (artikel 44, voorstellen (2017) 793 en 794).

3.8.3. **Het gebruik van het** nog op te stellen **Universal Message Format** (UMF) moet het hanteren van de nieuwe systemen, die verplicht zullen zijn, vergemakkelijken. Er zal in interfaces moeten worden voorzien in de lidstaten waar deze nog niet bestaan, alsook in een tijdelijk vertaalsysteem van de ene taal naar de andere.

3.9. *De bescherming van persoonsgegevens (artt. 7 en 8 van het Handvest):*

3.9.1. In de voorgestelde verordening wordt de mogelijkheid van veiligheidsincidenten erkend. De lidstaten en hun informatiesystemen moeten in eerste instantie de gegevensbeschermingsbeginselen in acht nemen die zijn neergelegd in de teksten, het Verdrag, het Handvest van de grondrechten en de algemene verordening gegevensbescherming ([12]), die op 25 mei 2018 in werking treedt.

4. **Discussie**

4.1. *Meerwaarde van interoperabiliteit in termen van democratie*

4.1.1. De Unie heeft behoefte aan regelgeving en onderzoeksmiddelen om zich tegen criminaliteit te beschermen. De interoperabiliteit van informatiesystemen biedt de mogelijkheid om de rechtsstaat te doen gelden en de mensenrechten te verdedigen.

4.1.2. *EES en ETIAS* zullen, in combinatie met het BMS en het CIR, het mogelijk maken om de grensovergangen van verdachte personen te controleren en om hun gegevens te bewaren. Dat rechtshandhavingsinstanties via het BMS mogelijk toegang zouden hebben tot niet-repressieve informatiesystemen op EU-niveau (artikel 17, CIR, voorstel (2017) 794 en 793)] is evenwel niet verenigbaar met de doelstellingen die als basis voor de voorstellen in kwestie zijn aangegeven. Het Comité (artikel 300, lid 4, VWEU) dient in dit verband te verwijzen naar het evenredigheidsbeginsel en dringt er bij de Commissie op aan om regelingen te vermijden van het type „Big Brother" ([13]), waarbij belemmeringen voor het vrije verkeer van Europeanen in het leven worden geroepen (artikel 3 VEU).

4.1.3. Het voorgestelde model voor de verzameling en het gebruik van persoonsgegevens die aan de grens en op het grondgebied van de Unie bij de controle van bewegingen en documenten zijn verkregen, wordt als waterdicht voorgesteld. Het zal alleen toegankelijk zijn voor bevoegde personen en voor veiligheids- en beheersdoeleinden, en zal tevens zorgen voor vlottere procedures.

4.1.4. Het EESC vraagt zich af of een waterdicht systeem wel realistisch is: er zullen nog lacunes blijven bestaan; de gefaseerde 9-jarige bouw is gebaseerd op „fundamenten" die nog niet bestaan, zoals de EES- of ETIAS-banken of de nationale interfaces. De technologische context is voortdurend in ontwikkeling, het project is noodzakelijkerwijs gebaseerd op de stand van de techniek en voorziet niet in een budget om de veroudering die zich in sommige digitale sectoren kan voordoen, te beheren.

([11]) Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

([12]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). EESC-adviezen: PB C 229 van 31.7.2012, blz. 90 en PB C 345 van 13.10.2017, blz. 138.

([13]) In *1984* van George Orwell.

4.1.5. Voorts had de snelle ontwikkeling van het gebruik van kunstmatige intelligentiealgoritmen (AI-algoritmen) in het project kunnen worden beschouwd als een instrument voor systeemcontrole en als een veiligheidssleutel die aan de besluitvormende autoriteiten moet worden toevertrouwd om het democratische gebruik van het systeem te garanderen.

4.1.6. In het voorstel wordt een systeem ontwikkeld voor bonafide, gezagsgetrouwe partijen. Het feit dat mensen de leiding hebben is geruststellend, maar zij kunnen ook de zwakke schakels zijn. Het Comité stelt voor een artikel toe te voegen waarin wordt voorzien in „differentieelschakelaars" in geval van een politieke en/of „beheerscrisis"; elk probleem in de databank kan een risico vormen voor het hele systeem ([14]). De veralgemening van het UMF zou kunnen leiden tot een zeer welkom internationaal gebruik ervan, dat voor de gegevensbescherming evenwel grote risico's met zich meebrengt. De bevoegde autoriteiten dragen een zware verantwoordelijkheid. Deze aspecten komen in de onderhavige teksten niet aan de orde.

4.2. *De bescherming van de grondrechten*

4.2.1. Grondrechten zijn absoluut; er kunnen alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang beantwoorden en indien de wezenlijke inhoud van de grondrechten wordt geëerbiedigd (artikel 8 en artikel 52, lid 1, van het Handvest van de grondrechten). Het Comité vraagt zich af hoe de proportionaliteit van de controlemaatregelen kan worden beoordeeld in het geval van migranten die op de vlucht zijn voor vervolging en in EU-kustgebieden asiel aanvragen (COM(2017) 794 final, Toelichting — Grondrechten). De opsporing van verdachten met het oog op het voorkomen van strafbare feiten, met name terroristische daden, **mag er niet toe leiden dat onze democratieën ontvankelijk gaan worden voor het begrip „anticiperende delicten"**; er moet onderscheid blijven tussen „activiteiten" die de openbare orde verstoren en „meningen".

4.2.2. Eerbiediging van de in het Handvest vastgelegde rechten moet zorgen voor een evenwicht tussen veiligheid en vrijheid; anders is de democratie ten dode opgeschreven. Het Comité is van mening dat dit evenwicht van cruciaal belang is en een permanente doelstelling moet zijn voor alle autoriteiten, met inbegrip van de toezichthoudende autoriteiten, op zowel nationaal als Europees niveau.

4.2.3. De keten van autoriteiten die betrokken zijn bij een zoekopdracht en de bijbehorende metagegevens zullen in het systeem worden opgeslagen. In geval van kwaadwillige inbreuk op de structuur en misbruik van de gegevens tussen het tijdstip van invoering en het tijdstip van verwijdering moeten de grondrechten van deze bevoegde autoriteiten zelf met betrekking tot de gegenereerde gegevens geëerbiedigd worden, met name wat betreft hun veiligheid en privacy.

4.3. *Gegevensbescherming*

4.3.1. In de voorstellen wordt het beginsel van bescherming van persoonsgegevens van meet af aan en bij verstek erkend, hoewel er in de toelichting op wordt gewezen dat dit volgens het Hof van Justitie geen absoluut voorrecht is. Het Comité erkent de voordelen van preventieve maatregelen om de veiligheid te waarborgen, valse identiteiten te bestrijden en het recht op asiel te waarborgen. Het wil evenwel ook wijzen op de grenzen van mathematisering en anonimisering van gegevens: de betrokkenen kunnen hun gegevens later nodig hebben.

4.3.2. Het benadrukt ook dat het soort opgeslagen gegevens (biometrische en biologische gegevens) voor bepaalde ondernemingen en voor criminaliteitsonderzoek van bijzonder belang is. Cyberveiligheid is in dit verband net zo belangrijk als fysieke veiligheid, en in de voorstellen wordt er te weinig over gezegd. De opgeslagen gegevens worden opgeslagen op een enkele fysieke locatie; zelfs beschermd, kan deze risico lopen.

4.3.3. Het EESC herinnert eraan dat de instellingen en organen van de EU ten aanzien van gegevensbescherming en het recht om gegevens te wissen (recht om te vergeten) Verordening 45/2001 moeten naleven, die minder bescherming biedt dan de Algemene verordening gegevensbescherming van 2016 ([15]) (die in mei 2018 in werking treedt) en door de lidstaten moet worden nageleefd. Het Comité wijst op de complexiteit van de toepassing van dit recht en vreest dat reizigers, migranten en asielzoekers niet in staat zijn dit recht te doen gelden:

1. de bescherming van persoonsgegevens moet in alle bestaande nationale en Europese databanken worden gevalideerd, zodat het geheel wordt beschermd;

2. het is van fundamenteel belang dat de burgers dit enorme netwerk van toezicht boven hun hoofd aanvaarden.

4.3.4. De bewaartermijn voor de door de bevoegde autoriteiten verzamelde gegevens wordt in de voorstellen niet duidelijk aangegeven. In de teksten wordt de procedure vermeld voor het recht op rechtzetting en/of verwijdering van gegevens, met een wisselwerking tussen de verzoekende en de verantwoordelijke lidstaat, maar worden geen termijnen vastgesteld voor de opslag van de gegevens (artikel 47 van de voorstellen). Het Comité beveelt aan om deze termijn vast te stellen en voor minderjarigen in te korten (Handvest, artikel 24), behalve in geval van terrorisme, zodat zij de kans krijgen om zich te integreren.

([14]) EDPS, bijlage, eindverslag van de deskundigengroep op hoog niveau, mei 2017.
([15]) Algemene verordening gegevensbescherming (Verordening (EU) 2016/679).

4.4. *Governance en verantwoordingsplicht*

4.4.1. Voor internationale gegevensbanken gelden niet dezelfde regels als voor Europese computersystemen. De vaststelling van een universeel toegangsformaat, dat internationaal zou kunnen worden, zal slechts een technisch element zijn dat de voorschriften niet eenvormig maakt, ook al moet Interpol artikel 17 van het VN-Verdrag ([16]) zeker naleven. Bovendien blijven de vergunningen onder de verantwoordelijkheid van de lidstaten vallen. Het EESC is van mening dat dit in de voorstellen aan de orde moet komen.

4.4.2. Een enkele zoekopdracht en de symbiose van Europese databanken zal tot een oordeel leiden. Het EESC wijst erop dat de gegenereerde administratieve lasten meer dan evenredig zullen zijn met de verworven snelheid. De Commissie zal zorgen voor goed bestuur in het kader van een controleprocedure met de lidstaten. Een sleutelrol zal zijn weggelegd voor het eu-LISA-agentschap, dat met name zal worden belast met het opzetten van procedures voor het verzamelen van informatie over de werking van de interoperabiliteit. Het agentschap zal informatie ontvangen van de lidstaten en Europol en om de vier jaar een technisch evaluatieverslag indienen bij de Raad, het EP en de Commissie, terwijl de Commissie een jaar later zelf een algemeen verslag zal opstellen (artikel 68 van de voorstellen). Voor het Comité gaat hier veel te veel tijd over. De beoordeling van de veiligheid van de interoperabiliteitsonderdelen (artikel 68, lid 5, onder d)) moet ten minste elk jaar plaatsvinden en die van het effect op de grondrechten ten minste om de twee jaar (artikel 68, lid 5, onder b)).

4.4.3. Het EESC betreurt het dat fundamentele kwesties zoals die welke in deze voorstellen aan de orde worden gesteld, worden beheerd door Europese agentschappen, waarvan de aanwervingsprocedures en het functioneren voor veel burgers ondoorzichtig zijn. Het is volgens hem zaak goede praktijken te vergelijken en alle onafhankelijke toezichthoudende autoriteiten voor gegevensgebruik (EDPS) en andere agentschappen, zoals FRA en ENISA, te raadplegen.

4.4.4. Al deze nieuwe structuren en procedures zullen worden ingevoerd door middel van gedelegeerde handelingen en uitvoeringshandelingen van de Commissie. Het Comité zou graag zien dat de doelstelling van eerbiediging van de grondrechten en bescherming van persoonsgegevens in de loop van de tijd in al deze besluiten verankerd blijft, als onderdeel van een aanpak om de opvang van personen aan de grenzen te verbeteren. Het EESC zou graag zien dat de Europese burgers worden geïnformeerd over de verschillende fasen van het project tot de voltooiing ervan, en dat zij educatieve informatie krijgen over de controles die zij moeten ondergaan.

5. **De noodzakelijke opleiding van toezichthoudende autoriteiten in de hele Unie**

5.1. In tegenstelling tot wat de Commissie in haar samenvatting van de effectbeoordeling (C) stelt, zullen er volgens het Comité in de eerste periode (na 2021) veel opleidingscursussen nodig zijn. Het gaat om 76 miljoen EUR per jaar. De overgang naar nieuwe procedures vereist altijd een upgrade. Dit betreft alle grenzen van de Unie en de nationale systemen. Sommige lidstaten beschikken nog niet over compatibele systemen en zullen een grote inspanning moeten leveren en interfaces moeten opzetten die hen in staat stellen deel te nemen. Om interoperabiliteit mogelijk te maken moeten de verschillen tussen de lidstaten worden weggewerkt.

5.2. Opleiding in het gebruik van kwaliteitsgegevens en het UMF is van essentieel belang. Het Comité stelt voor om samen met Cepol ([17]), Frontex, Europol enz. een gemeenschappelijk opleidingscentrum voor de bevoegde autoriteiten op te richten, met inbegrip van eu-LISA, waarvan de bevoegdheden streng moeten worden gecontroleerd.

5.3. Een instrument als de MID bestaat nergens anders. Als het instrument succesvol is, zal het krachtig zijn. Het nieuwe systeem vereist gegevens van de hoogste kwaliteit. Om ervoor te zorgen dat het hele project aan de verwachtingen voldoet, moeten alle lidstaten op hetzelfde niveau deelnemen, anders zullen de tekortkomingen ernstiger zijn dan voorheen. In dat geval zouden het asielrecht en het recht op toegang tot internationale bescherming worden ondermijnd (artt. 18 en 19 van het Handvest).

6. **De financiering**

6.1. De voorgestelde architectuur is gebaseerd op een aantal veronderstellingen: de goedkeuring door de besluitvormende autoriteiten van de systemen *EES* en *ETIAS*, het *UMF*, de goede werking van de *MID* en de beveiliging van het *CIR*. Zullen de EDPS en het eu-LISA-agentschap met z'n tweeën, en misschien ook het ENISA-agentschap, over voldoende personele en financiële middelen beschikken? De Commissie stelt cofinanciering voor tussen de EU en de lidstaten. Het Comité stelt vast dat het „semester" nog steeds met bezuinigingsbegrotingen wordt beheerd en dat het huidige gebruik van de bestaande databanken (SIS, VIS, Prüm, *EES*) nog moet worden geoptimaliseerd overeenkomstig de wettelijke vereisten (verslag van de deskundigengroep).

([16]) Internationaal Verdrag inzake burgerrechten en politieke rechten, VN: „Artikel 17: 1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam. 2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting."

([17]) Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Boedapest, Hongarije)

6.2. Het EESC plaatst vraagtekens bij de gevolgen van de brexit voor de begroting, hoewel het Verenigd Koninkrijk geen deel uitmaakt van het Schengensysteem. Meer in het algemeen vraagt het zich af hoe complex het in de toekomst zal zijn om de interoperabiliteit te beheren in Europese landen die niet aan het SIS maar aan andere databanken zoals Eurodac deelnemen.

6.3. Het geplande fonds is het ISF, het Fonds voor interne veiligheid en grenzen. De inwerkingtreding is gepland voor 2023. Het Comité vraagt zich af of vijf jaar voldoende is om de Europese verschillen te verkleinen en aan de voorwaarden voor succes te voldoen. De geplande begroting bedraagt 424,7 miljoen EUR over een periode van 9 jaar (2019-2027). De Unie (FSI) en de lidstaten zullen moeten betalen. Staten moeten ervoor zorgen dat de bestaande systemen goed kunnen functioneren met de nieuwe informatica-architectuur. De Commissie is van mening dat het herstel van de groei moet worden gebruikt om deze investeringen te doen.

Brussel, 23 mei 2018.

De voorzitter
van het Europees Economisch en Sociaal Comité
Luca JAHIER