European Economic and Social Committee

SOC/573
Interoperability package

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226
[COM(2017) 793 final – 2017/0351 (COD)]
Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)
[COM(2017) 794 final – 2017/0352 (COD)]

Rapporteur: **Laure BATUT**

Consultation	European Commission, 19/01/2018
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Section for Employment, Social Affairs and Citizenship
Adopted in section	25/04/2018
Adopted at plenary	23/05/2018
Plenary session No	535
Outcome of vote (for/against/abstentions)	160/3/2

1. Conclusions and recommendations

1.1 The EESC considers the European Commission's proposal for improving interoperability between EU information systems for borders and visas and for police and judicial cooperation, asylum and migration to be useful and positive.

1.2 In the EESC's view, this interoperability needs to be a strategic objective for the EU, in order for the Union to continue to be an open area that safeguards fundamental rights and mobility. The EU and the Member States have an obligation to protect the lives and the safety of all human beings, and the principle of non-refoulement should be fully respected.

1.3 There will be more understanding for these interoperability measures if they:

- ensure, as part of the EU's migration strategy, a balance between freedom and security in accordance with the separation of powers;
- safeguard the fundamental rights of the people concerned, in particular the protection of their personal data and privacy and their right of access to and correction and erasure of their data within a reasonable time, via accessible procedures;
- reiterate, including in all the implementing texts, the requirement of including data protection principles from the design stage ("privacy by design");
- do not create new barriers to the normal flow of passengers and freight.

1.4 The EESC calls for the procedures and guarantees regarding the use of data for law enforcement purposes to:

- provide for application of the most protective European law (GDPR);
- speed up the process by which the Member States responsible reach decisions on applications for international protection;
- safeguard the right of the people concerned to judgments in a two-tier court system;
- ensure that minors, and in particular unaccompanied minors – whether they are in an irregular situation, are being persecuted or have committed crimes – have the right to obtain a visa, to be protected and integrated and to exercise the right to be forgotten in a shorter period than for adults.

1.5 The EESC believes that the current legal basis for these information systems should be strengthened, and should take into account the upgradeability of data collection systems. It recommends:

- enhancing the security of existing databases and of their communication channels;
- assessing the impact on risk management of strengthening ex ante controls;
- ongoing monitoring and evaluation of the architecture by the data protection authorities (EDPS); it requires the parties responsible to report annually to the decision-making authorities and to the Commission regarding the security of the interoperability components, and every two years on the impact of the measures on fundamental rights.

1.6 The EESC feels that the project needs to rely on skilled staff, and recommends:

- robust training programmes for the authorities concerned and eu-LISA staff;
- strict checks on the competences of staff of and applicants for that agency.

1.7 The EESC has concerns about the funding for the new system. It is crucial to follow up on the planning in order to avoid budget slippage and see the project through to the end in 2029.

1.8 The EESC recommends that the public should be kept informed of progress on the project until its completion, and that people should be given educational information on the checks to which they will be subject. It considers that the possibility must be available of halting the whole project if freedom and fundamental rights were to be threatened by abuse of the system.

2. Introduction

2.1 In the international context of 2017, considered as unstable in terms both of geopolitics and of the internal security of the Member States, the Council has on several occasions asked the Commission to introduce the means of tracing persons deemed to be a "risk" who have already been subject to monitoring in one of the Member States. Identifying their border crossings and their movements within Europe could be crucial for security in the EU.

2.2 In its Resolution of 6 July 2016, the Parliament called on the Commission to provide the necessary data protection safeguards.

2.3 The texts under consideration fall under the objective of "preserving and strengthening Schengen"[1]. The EU already has several sets of rules and digital information services in areas linked to checking the border crossings of persons and goods.

2.4 As a reminder:

- **SIS: Schengen Information System**, one of the oldest mechanisms, since revised, which manages a broad range of alerts concerning people and goods;
- **Eurodac: European system for comparing the fingerprints** of asylum seekers and third-country nationals in an irregular situation at borders and in the Member States, and for determining the Member State responsible for applications (EESC-2016-02981, rapporteur: Mr Moreno Díaz[2]);
- **VIS: Visa Information System** (Visa Code), which manages visas for short stays (EESC-2014-02932, rapporteurs: Mr Pezzini and Mr Pariza Castaños[3]);

1 COM(2017) 570 final.

2 OJ C 34, 2.2.2017, p. 144.

3 OJ C 458, 19.12.2014, p. 36.

- **EES: Entry-Exit System**, currently awaiting decision, which should electronically manage the passport details and entry/exit dates of third-country nationals visiting the Schengen area (EESC-2016-03098, SOC/544, rapporteur: Mr Pîrvulescu[4]);
- **ETIAS: European Travel Information and Authorisation System**, currently awaiting decision, which should be a large automated system for storing and verifying ex-ante the data of third-country nationals who do not require a visa to travel within the Schengen area (EESC-2016-06889, SOC/556, rapporteur: Mr Simons[5]);
- **ECRIS-TCN: European Criminal Record Information System for third-country nationals**, as currently proposed by the Commission, a digital system for exchanging information on judgments already handed down by national courts.

2.5 The current tools of an authorised authority can be likened to a smartphone with different applications, each of them separate and providing its own information.

2.6 Aside from the SIS, these systems are focused on **managing third-country nationals**. There are six complementary, decentralised systems. The search results are the sum of the different responses obtained from the various databases by the investigation services, depending on their access rights.

2.7 The Commission intends to address the following question:

– what method to use, without changing the structures already in place or losing complementarity between them, to harmonise queries to all the databases at the same time in order that, at a single point of entry into EU territory and using a single query of the system, all information gathered in existing databases will be available to the supervisory authority authorised to query them, while simultaneously respecting the rules on data protection and fundamental rights.

2.8 In the present proposals the European Commission

2.8.1 would like to add the additional possibilities that would be created by access to the Europol and Interpol databases, which already cooperate with the European supervisory authorities;

2.8.2 would like to "synchronise" information searches in order to reduce the response times with regard to migrants' cases, and to speed up the security response when necessary. To do this, it proposes creating new bodies that would allow the current databases to work together.

2.9 **Its objectives are to plug as many gaps in the various systems as possible, improve the** management of the outer borders of the Schengen area, contribute to internal security in the EU, manage identity fraud, tackle cases of multiple identities, find suspected or convicted persons and check their identity within the Schengen area.

4 OJ C 487, 28.12.2016, p. 66.

5 OJ C 246, 28.7.2017, p. 28.

2.10 To continue with the image of the smartphone, not only would the authorised authority have many applications at its disposal, it would also be able to gather together – simultaneously, through a single search, and by using his/her access codes – data stored on all types of device: PC, laptop, mobile phone, tablet, etc.

3. Functioning of the system

3.1 The Commission has held consultations and convened a High Level Expert Group on Information Systems and Interoperability[6], appointed by the Member States, the countries of the Schengen group, European agencies such as eu-LISA[7] and the FRA[8], coordinated by DG Home.

The method: interconnectivity or interoperability?

3.1.1 The **interconnectivity** of information systems means the possibility of interlinking them so that the data held by one system can be consulted automatically by another.

3.1.2 **Interoperability**[9] is the ability of systems to communicate, exchange data and use the information which has been exchanged, in accordance with the authorisations granted to the systems.

3.2 Choosing interoperability

3.2.1 The Commission takes the view that this does not interfere with existing structures and competences, and that the data will remain "in compartmentalised silos". Despite the increase in transmission possibilities, this could be a security advantage for systems and data, none of which would obviously be accessible via the internet. The documents to which the opinion relates contain significant similarities;

- one of them, COM(2017) 793, relates to the interoperability of information systems for borders and visas;
- the other, COM(2017) 794, relates to police and judicial cooperation, asylum and migration.

3.3 New tools

3.3.1 In order to function based on interoperability, the six databases will need to be complemented by four new tools in order to work quickly by only submitting a single query to the system, ensuring that requests always originate from authorised persons.

---

6 DG Home, Unit B/3; Commission Decision C/2016/3780 of 17 June 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=EN

7 European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

8 EU Agency For Fundamental Rights

9 Commission communication, COM(2016) 205 final, "Stronger and Smarter Information Systems for Borders and Security"

3.4 **The European Search Portal (ESP)**

3.4.1 The authorised supervisory authority (end-user) should have a single access to the whole system. Instead of carrying out six searches, only one would be carried out (police, customs, etc.), to query several databases simultaneously concerning the requested data, without storing any of it. If the data exist, the system will find them. In the case of suspected criminal or terrorist activity, the first search for the person being checked may not yield any results ("no-hit"), but if a match to the data is found ("hit") in databases such as SIS, EES or ETIAS, this may lead to more in-depth searches and an inquiry.

3.5 **Shared Biometric Matching Service (Shared BMS)**

3.5.1 This shared matching platform will make it possible to simultaneously search for and compare data converted into mathematical representations, biometric data, fingerprints and photographic ID from the various databases, such as SIS, Eurodac, VIS, *EES*[10] and *ECRIS*, but not *ETIAS*; the data they contain will therefore need to be compatible.

3.5.2 The data converted into a mathematical representation will not be preserved in their original form.

3.6 **Common Identity Repository (CIR)**

3.6.1 A common identity repository will gather data concerning the biographical and biometric identity of third-country nationals who have been checked, whether they are at the border or within Member States (Schengen). An indicator showing a match between information in the various databases will speed up searches. Under the responsibility of eu-LISA and using its security resources, these data will be stored in a way that means that no person can have access to more than one alphanumeric line at a time. Developed on the basis of the EES and the ETIAS, the CIR should avoid data duplication. It will also be possible to use the repository for civilian research.

3.7 **Multiple-Identity Detector (MID)**

3.7.1 The role of the multiple-identity detector will be to verify the correct identity of bona fide persons and to combat identity fraud, by searching all databases at the same time. As yet, no administration has used a tool like this, which should help to avoid identity theft.

3.8 **The role of the eu-LISA agency**[11]

3.8.1 The agency, set up in 2011, aims to support EU policies in the fields of justice, security and freedom. Based in Tallinn in Estonia, it already provides for exchange of information between

10 The italics serve as a reminder that the texts relating to these bodies have not yet been adopted.

11 Regulation (EU) No 1077/2011, eu-LISA, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

the Member States' law enforcement authorities, and ensures seamless operation of large-scale IT systems and the freedom of movement of people within the Schengen area.

3.8.2 It works on the Smart Borders project and, under the new data exchange architecture, its role will involve storing information linked to individuals, e.g. information relating to the authorities, investigations and investigators. It will check the authorisations of those making requests and ensure data security, including in the event of a "security incident" (Article 44 of proposals COM(2017) 793 and 794).

3.8.3 **Use of the Universal Message Format** (UMF) – which is still to be created – should make it easier to work with the new systems, which will be compulsory, making it necessary to create interfaces in the Member States which do not yet have one and a system for temporary translation from one language into another.

3.9 **Protection of personal data** (Articles 7 & 8 of the Charter):

3.9.1 The proposal for a Regulation recognises the possibility of security-related incidents. The Member States and their data systems must in the first instance comply with the data protection principles laid down in the texts, the Treaty, the Charter of Fundamental Rights, and the GDPR[12] which will enter into force on 25 May 2018.

4. Discussion

4.1 Added value of interoperability in terms of democracy

4.1.1 The EU needs regulation and investigative resources that protect against crime. Interoperability of information systems is an opportunity to assert the primacy of law and the protection of human rights.

4.1.2 The *EES and ETIAS* in conjunction with the BMS and CIR will make it possible to monitor border crossing by people under suspicion, and to retain their data. However, the possibility of "access [via the BMS] by law enforcement authorities to non-law enforcement systems at EU level" (Article 17 on the CIR, proposals COM(2017) 793 & 794) cannot be compatible with the objectives set out as the basis for the proposals in question. The Committee (Article 300(4) TFEU) must draw attention here to the principle of proportionality, and urges the Commission to avoid any "Big Brother[13]"-style system and to avoid creating barriers to the free movement of European citizens (Article 3 TEU).

4.1.3 The proposed model for the collection and use of personal data obtained at the border and within EU territory when monitoring movements and the documents held is presented as being

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EESC opinions: OJ C 229, 31.7.2012, p. 90 and OJ C 345, 13.10.2017, p. 138.

13 In *1984* by George Orwell.

watertight, open only to authorised persons for security and management purposes, and will make the procedures smoother.

4.1.4 The Committee has doubts about how watertight it really is: shortcomings will still remain, and the structures will be built up over nine years, based on "foundations" that do not yet exist, such as the EES and ETIAS databases and national interfaces. The technology is constantly evolving, but the project is necessarily based on the state of the art and has no budgetary provision for managing the obsolescence that may emerge in some digital sectors.

4.1.5 Moreover, the rapid growth in the use of artificial intelligence (AI) algorithms could have been considered in the project, both as a system monitoring tool and as a security key that can be given to the decision-making authorities to ensure the democratic use of the architecture.

4.1.6 The proposal sets out a system for law-abiding players acting in good faith. The fact that people are in the driving seat is reassuring, but they can also be the weak links in the chain. The Committee suggests adding an article providing for "circuit breakers" in the event of a political or "management" crisis, as any problem in one database could present a risk to the entire structure[14]. Wider application of the UMF could result in international use, which would be very positive but present risks in terms of data protection. The authorised authorities will bear a heavy responsibility. These aspects are not considered in the texts under discussion.

4.2 **Protection of fundamental rights**

4.2.1 Fundamental rights are absolute: they may only be subject to limitations that are necessary and genuinely meet objectives of general interest recognised by the Union, and only if their essence is respected (Articles 8 and 52(1) of the Charter of Fundamental Rights). The Committee wonders how the proportionality of control measures can be assessed in the case of migrants fleeing persecution and seeking asylum on the EU's coasts. (COM(2017) 794, p. 17 – explanatory memorandum). Looking for suspects in order to prevent criminal – including terrorist – acts **must not bring our democracies closer to the concept of "pre-crime"**; there must still be a distinction between "activities" that violate public order and "opinions".

4.2.2 Respect for the rights set out in the Charter for all people must safeguard the balance between security and freedom without which democracy dies. In the Committee's view, this balance is crucial and should be a permanent objective for all authorities, including supervisory authorities at both national and European level.

4.2.3 The chain of authorities involved in a search, and the associated metadata, will be stored in the system. The fundamental rights of the authorised authorities themselves must also be respected with regard to the data generated, in particular with regard to their security and privacy, in the event of malicious intrusion into the structure and misuse of data between the times of capture and deletion.

14 EDPS, Annex to the High Level Expert Group Final Report, May 2017

4.3 **Data protection**

4.3.1 The proposals recognise the principle of data protection by design and by default, even though the explanatory memoranda point out that, according to the Court of Justice (ECJ), this is not an absolute right. The Committee recognises the benefits of preventive measures that ensure safety, of combating false identities and of guaranteeing the right to asylum, but it stresses that anonymising and generating mathematical representations of data have their limitations: the people concerned may subsequently need their data.

4.3.2 It also stresses that the types of data retained – biometric and biological – are of particular interest for certain businesses and for criminals. In this context, cybersecurity is just as important as physical security, and there is too little mention of it in the proposals. The stored data will be kept in a single physical location; however well protected it is, it could still be exposed.

4.3.3 The EESC points out that, when it comes to data protection and the right to erasure (right to be forgotten), EU institutions and bodies must comply with Regulation (EC) No 45/2001, which provides less protection than the GDPR[15] of 2016 (to enter into force in May 2018) that the Member States must follow. The Committee highlights the complexity of implementing this right, and is concerned that travellers, migrants and asylum seekers will not be in a position to enforce it:

1) data protection must be validated for all existing national and European databases in order to ensure that the whole system is protected;
2) it is absolutely vital in order for the public to accept this vast surveillance network over their heads.

4.3.4 The retention period for data gathered by the authorised authorities is not clearly defined in the proposals. The texts set out the procedure for correction and/or erasure – which goes back and forth between the Member State to which the request has been made and the Member State responsible – but does not set time limits for retaining data (Article 47 of the proposals). The Committee recommends that such a time limit should be set, and that it should be shorter for minors (Article 24 of the Charter), except in cases of terrorism, so that they can have a chance of integration.

4.4 **Governance and accountability**

4.4.1 International databases are not subject to the same rules as European computer systems. The establishment of a universal access format, which could become increasingly international, would be just one technical element that would not unify the regulations, even though Interpol must of course respect Article 17 of the UN Covenant[16]. Moreover, authorisations will remain a

15 General Data Protection Regulation (Regulation (EU) No 2016/679)

16 International Covenant on Civil and Political Rights – UN – "Article 17: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

matter for the Member States. The EESC believes that this issue should be addressed in the proposals.

4.4.2 Just a single query, and the symbiosis of European databases will give its verdict. The EESC emphasises that the bureaucracy generated will be more than proportionate to the speed gained. Governance will be provided by the Commission as part of a control procedure together with the Member States. The fulcrum will be the eu-LISA agency, which is responsible inter alia for establishing the procedures for gathering information on how interoperability is working; it will receive information from the Member States and Europol, and present a technical evaluation report to the Council, European Parliament and Commission every four years, with the Commission publishing its own overall report a year later (Article 68 of the proposals). In the Committee's view, this interval is much too long. The assessment of the security of the interoperability components (Article 68(5)(d)) should be made at least once a year, and the examination of the impact on fundamental rights (Article 68(5)(b)) should be undertaken at least every two years.

4.4.3 The Committee finds it regrettable that issues as fundamental as those addressed in these proposals will be managed by European agencies, whose recruitment and operation are obscure to many citizens. It considers it necessary to compare best practices and to consult all independent data use supervisory authorities (EDPS) and other agencies such as the FRA and ENISA.

4.4.4 All of these new structures and procedures will be put in place by means of Commission delegated acts and implementing acts. The Committee hopes that the objectives of respecting fundamental rights and protecting personal data will continue to be enshrined in all of these acts over time, in an approach focusing on improving reception of people at borders. The EESC recommends that the European public should be kept informed of the stages towards completion of the project, and that people should be given educational information on the checks to which they will be subject.

5. The necessary training of supervisory authorities throughout the EU

5.1 In the Committee's view, a lot of training will be needed in the first period (after 2021), contrary to what the Commission claims in its impact assessment summary (C). It mentions a figure of EUR 76 million per year. The transition to new procedures always calls for upgrades. All EU borders and national systems are concerned here. Some Member States still do not have compatible systems and will need to make considerable efforts and set up interfaces that enable them to participate. In order for interoperability to work, the disparities between Member States will need to be ironed out.

5.2 Training on the use of high-quality data and the UMF will be necessary. The Committee suggests that a joint training hub for authorised authorities, including eu-LISA – the competences of whose members should be carefully verified – should be organised with CEPOL[17], Frontex, Europol, etc.

17 European Union Agency for Law Enforcement Training (Budapest, Hungary)

5.3 A tool like the MID does not exist elsewhere. If successful, it would be a powerful tool, The new architecture will require the highest possible data quality. To ensure that the project as a whole meets expectations, all Member States must be able to participate at the same level, otherwise the gaps will be even bigger than they were before – which would undermine the right to asylum and to access international protection (Articles 18 and 19 of the Charter).

6. Financing

6.1 The overall architecture proposed is based on certain assumptions: that the decision-making authorities will adopt the *EES*, *ETIAS* and *UMF* systems, that the *MID* will work properly and that the *CIR* will be secure. Will two bodies – the EDPS and the eu-LISA agency, and perhaps ENISA as well – have sufficient staff and financial resources? The Commission is proposing EU/Member State cofinancing. The Committee notes that management of the "Semester" is still based on austerity budgets and that, in addition, the current use of existing databases (SIS, VIS, Prüm, *EES*) still needs to be optimised in accordance with the legal requirements (report from the expert group).

6.2 The EESC wonders what budgetary impact Brexit will have, although the United Kingdom is not in the Schengen system, and more generally about the complexity of managing interoperability in the future in European countries that do not use the SIS but do participate in other databases such as Eurodac.

6.3 The proposed fund is the ISF, the Internal Security Fund for borders. It is scheduled to start operating in 2023. The Committee questions whether five years will be long enough to reduce the disparities in Europe and to establish the conditions for success. The proposed budget is EUR 424.7 million over nine years (2019-2027), to be paid by the EU (ISF) and the Member States. The Member States must put themselves in a position to ensure that the current systems work properly with the new IT architecture. The Committee believes that the return to growth should help with the implementation of these investments.

Brussels, 23 May 2018

Luca JAHIER
The president of the European Economic and Social Committee