Meijers Committee
standing committee of experts on international immigration,
refugee and criminal law
[redacted]

CM1802 Comments on the 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) 12 December 2017, COM (2017) 794

19 February 2018

1. Introduction

According to the proposal for a Regulation on interoperability (further: the proposal), national authorities will be able to check whether information on an individual person is recorded in one of the EU databases (VIS, SIS II, Eurodac, the Entry/Exit System (EES), the proposed ETIAS, and the proposed ECRIS-TCN). This access is based on four mechanisms:

First, the European Search Portal (ESP) will serve as a 'message broker' enabling user to detect whether information on an individual third country national is available in one of the EU large-scale databases. Second, the use of a shared biometric matching service (shared BMS) enables the querying and comparison of biometric data (fingerprints and facial images) from several central systems (in particular, SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN system). Third, a common identity repository (CIR) is to be used for storing biographical and biometric identity data of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. Fourth, the multiple-identity detector (MID) would enable verification if the queried identity data exists in more than one system.

According to the Explanatory Memorandum, the proposal will not change that each of these five central systems records or will record biographical data on specific persons for specific reasons: the relevant identity data would be stored in the CIR but would continue to 'belong' to the respective underlying systems that recorded this data.

The central objectives of this proposal as described in the Explanatory Memorandum (p. 3) are:

(1) ensure that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities, have fast, seamless, systematic and controlled access to the information that they need to perform their tasks;

(2) provide a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of *bona fide* persons and combating identity fraud;

(3) facilitate identity checks of third-country nationals, on the territory of a Member State, by police authorities; and

(4) facilitate and streamline access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.

2. General comments

In general, the current architecture of databases and their interconnections[1] is growing more complex by the day. This development is not necessarily in the interest of border control, immigration and law enforcement. This is how this proposal for interoperability is justified.

In addition, this complexity is not necessarily in the interest of the individual whose data is included in one or more of these databases either. This complexity make it increasingly difficult for an individual (an EU citizen or a third country national) or his or her representative to gain insight in the data that are stored on him or her in these different databases. Moreover, how can the accuracy and the quality of this data be safeguarded?

The Meijers Committee underlines that the public interests and the interests of individuals included in these data bases may very well concur. The accuracy and the quality of personal data serves all objectives.

Nevertheless, it is important to assess the proposed regulation on interoperability also from the perspective of the individual and to consider the individual's interests as an objective for introducing the new interoperability mechanism.
A specific issue in this context relates to the fact that the proposal concerns the interoperability of systems which do not only have different purposes, but also include different categories of data subjects.[2] The systems include data of individuals because they are linked to criminal behaviour or illegal border crossing, as well as bona fide persons (included in Eurodac and VIS). It should be explained interoperability will not lead to the mixing up of these categories.

Since the proposal allows for the use of a shared BMS enabling the querying and comparison of biometric data (fingerprints and facial images), the Meijers Committee questions how the proposal relates to the existing exchange of information in accordance with the Prüm Decision.[3] This decision provides for decentralised system for the exchange of biometric data for law enforcement purposes. At the very least, it should be explained why this proposal is a necessary complement to the Prüm Decision.

The security of the interoperability components as such should be safeguarded keeping in mind that even though these components do not store data, they can still be vulnerable for manipulation with malice intent.

3. Non discrimination

---

1 For an overview of the information exchange environment in the justice and home affairs area, see Council, 6253/17, 15.02.2017.

2 Making a clear distinction between personal data of different categories of data subjects is a requirement of Article 6 of, Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.

3 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

The proposal enhances the risk of discrimination of third country nationals and of persons of racial or ethnic origin. Article 5 of the proposal on non-discrimination, which only applies to data processing, does not take away the discriminatory nature of the proposal itself, nor the possible discriminatory effect of specific checks on third country nationals, based on this interoperability-mechanism.

With regard to the purpose of the proposal to facilitate and streamline access to EU databases for law enforcement authorities, questions arise on the necessity and proportionality of this differential treatment between, on the one hand EU citizens, and on the other hand, third country nationals (including family members of EU citizens, asylum seekers, and Schengen visa applicants).

Specifically, the explanatory memorandum emphasizes this differentiated treatment between EU citizens and third-country nationals in view of the goal of preserving security in the EU: 'Whilst not directly affecting EU nationals (the proposed measures are primarily focused on third-country nationals whose data is recorded in an EU centralised information system), the proposals are expected to generate increased public trust by ensuring that their design and use increases the security of EU citizens.'[4] This justification basically means that third country nationals should be subject to additional security checks - even if there is no connection to any illegal behaviour - in order to make EU citizens feel more secure.

Furthermore, the explicit objective of the proposal of facilitating identity checks of third country nationals by police organisation within the EU territory, to see whether information on this person is stored in one or more of the EU databases, will enhance the possibility of third-country nationals (or those considered to be third-country nationals) being stopped for identity checks.

In this context, the Meijers committee recalls the case *Huber v. Germany*, in which the CJEU dealt with the differential treatment between nationals and EU citizens living in Germany with regard to the central storage and multiple use of personal data in an aliens administration, including the use for law enforcement purposes.[5]

According to the CJEU, such differentiation was in breach of the right to non-discrimination in relation to data protection rights, including the principle of purpose limitation. As the fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of the nationality of their perpetrators, the CJEU found that, 'as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory'.

This reasoning of the CJEU equally applies to the aforementioned different treatment based on nationality with regard to the central storage of copies of travel documents for other purposes than those which are directly related to migration control purposes.

4. General observations on data protection

In the explanatory memorandum, it is submitted that data protection standards are met, however without substantiating how this proposal meets these standards (which are laid down in Article 8 of

4 COM (2017) 794, page 17 .
5 CJEU *Huber v. Germany,* C-524/06, 16 December 2008, para 78-79.

the Charter of the fundamental rights and in the legal instruments of the EU based on Article 16 TFEU), even though the impact on the right to personal data protection of Article 8 is extensively described in the Commission's Impact Assessment.[6] The Meijer Committee observes that the proposal should be supported by an assessment of the proportionality of the interference with the right to data protection, as required by Article 8 and Article 52 (1) of the Charter and developed by the CJEU.[7]

It is furthermore unclear how the proposal interacts with the general data protection regulation (GDPR)[8] and directive 2016/680 (data protection for police and justice).[9] Considering the different databases involved and the purpose the data are processed for (which does not change by the fact that the databases become interoperable), the question should be answered when the GDPR is applicable and when the directive on data protection for police and justice.

With regard to the centralised parts of the systems, it is also unclear how the proposal relates to the proposal for a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.[10]

Finally, the Meijers Committee submits that the processing of personal data required by the proposal, is likely to result in a high risk to the rights and freedoms of natural persons. This should be specified in a provision or a recital proposal, with an Article 35 of the GDPR and/or Article 27 of the directive and/or to the relevant article in the new data protection regulation for EU institutions and bodies.

5. Specific data protection related issues

Purpose limitation
According to the explanatory memorandum, access 'to data is reserved exclusively for duly authorised staff of the Member State authorities or EU bodies that are competent for the specific purposes of each information system and limited to the extent that the data are required for the performance of tasks in accordance with these purposes.'[11]

The proposal as such does not alter the specific purposes of the EU databases involved. However, on the basis of the proposal, every designated authority of Member States will be able, via the European Search Portal, to learn about the fact that information on a third-country national is stored in one of the EU databases. In other words, the access of authorities to the European Search Portal is not restricted to their specific competence or task, whereas this specific competence or task currently limits their access to the specific EU databases. Therefore, information retrieved via the European Search Portal will establish that somebody is included in, for example, Eurodac or in SIS II. This implies a widening of the purpose of these databases: even if access to the personal file in this

6 SWD(2017) 473 final, 12.12.2017, p. 34-44.
7 See e.g. Joint cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238.
8 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)OJ L 119/1. .
9 See footnote 2.
10 Council, 15961/17, 22.12.2017.
11 COM (2017) 794, page 19.

database is not allowed because lack of authorisation, the authority will have gained knowledge of the existence of the file.

Moreover, the mere knowledge that a person's data are included in a particular database gives an authority a view of that person's actions, which can in itself be an interference with the right to data protection laid down in Article 8 of the Charter (and with Article 7 of the Charter on the right to privacy). This requires that the proportionality of this access should be assessed.

We further would like to raise a specific question: if the proposal as such does not increase or change the authorities having access to each individual EU database, what is the meaning of Article 43 on the confidentiality of SIS data?[12] As this confidentiality is already safeguarded in SIS II Regulation and SIS II Decision for those authorities granted access to the different categories of alerts in SIS, it should not be necessary to repeat a provision on confidentiality in this proposal. However the wording in Article 43, on applying rules of secrecy and confidentiality for 'all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law' implies that the proposal will allow access to categories of SIS for other persons and bodies, than currently authorised under the SIS Regulation and SIS II Directive. Further clarification is needed on the reason why Article 43 only applies to SIS data and does not contain a specific rule on confidentiality applicable to the complete system.

Data retention
Currently, EU law provides for different time limits for the retention of personal data included in the different EU databases (Eurodac 10 and 2 years, VIS 5 years, SIS II: 3 years with possibility of extension).

The proposal does not change these time limits as such. However, the proposal is less clear with regard to which specific data retention periods applies from the moment information is held via the CIR. According to Article 23 of the proposal, 'The individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the information systems whose data is contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data.'[13]

This implies that the data retention period is tied to the time limit which allows the longest time of data retention. So if, for example, on the basis of the VIS Regulation information on a visa applicant should be deleted from VIS, and his/her fingerprints are also stored in Eurodac, the person's information may remain for more than 5 years in CIR, including the information that a file was stored into VIS on this person. This changes the specific data retention periods as indicated, which is not in accordance with the data retention provisions provided for by the specific legal instruments setting up the relevant databases or with the data retention principle embedded in Article 5, 1, e) of the GDPR and Article 4, 1, e) of the directive on data protection for police and justice.

[12] 'Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.'

[13] COM (2017) 794, page 47.

Supervision by independent data protection authorities
In many Member States, national Data Protection Authorities are understaffed. This proposal adds another, difficult, and technically very complicated supervision task to the long list of tasks of these authorities. We recall that Article 57 GDPR already contains mandatory 22 tasks for these authorities,

The keeping of logs as proposed in Article 24 of the proposal is an important tool to control access to data files. However, implementation of data retention periods, security of data, prevention against unauthorised use, etc., requires effective and accessible control and supervision mechanisms. Article 49 (2) of the proposal requires the Member States to ensure the necessary resources. This requirement is an addition – for these additional tasks – to the similar provisions included in Article 52, 4 GDPR and in Article 42, 4, of the directive on data protection for police and justice. The Meijers Committee recommends that the European Commission (or the European Data Protection Board) specifies how Article 49 (2) of the proposal should be implemented.

Right of access, correction, or deletion
The Meijers Committee questions how an effective implementation of the rights to have access to, and correction and deletion of their data, as provided in Article 47 of the proposal, can be guaranteed. Current practices with regard to SIS II and the right of individuals in SIS, already establish that in Member States (and national data protection authorities are involved) it is difficult for individuals confronted with the use or effects of such a database, to enforce these rights[14] This problem is likely to increase where based on the interoperability proposal even more databases, authorities are involved.

The Meijers Committee also questions the effective remedies and the access to justice for individuals whose data are unlawfully processed. Article 47 of the proposal mentions that individuals have a right to address the Member State responsible but does not specify what action an individual should take when a so-called red link is made incorrectly.

Furthermore, the time limits as provided in Article 47 of the proposal must be considered long: for responding to a request for access 45 days, and with regard to requests for correction or deletion, seven days to contact the responsible Member State and 30 days for the responsible Member State to respond. The proposal does not provide any further provision on the consequences for Member State of not responding or acting in time.

The Meijers Committee recommends that these issues will be addressed during the legislative procedure.

---

[14] E. Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden-Boston: Martinus Nijhoff Publishers, 2008. See moreover: European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the Area of Freedom, Security and Justice, 17 November 2017.