Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2018/C 233/07)

Today's pressing challenges related to security and border management require smarter use of the information already available to competent public authorities. This has prompted the European Commission to launch a process towards the interoperability of (existing and future) EU large-scale information systems in the fields of migration, asylum and security. In December 2017, the Commission issued two Proposals for regulations that would establish a legal framework for interoperability between EU large-scale information systems.

Interoperability, provided that it is implemented in a well-thought manner and in full compliance with the fundamental rights, including the rights to privacy and to data protection may be a useful tool to address legitimate needs of competent authorities using large-scale information systems and to contribute to the development of effective and efficient information sharing. Interoperability is not only or primarily a technical choice but rather a political choice liable to have profound legal and societal consequences that cannot be hidden behind allegedly technical changes. The decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'.

While interoperability might have been envisaged initially as a tool to only facilitate the use of the systems, the Proposals would introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks, as well as streamline access to non-law information systems by law enforcement authorities.

In particular, the Proposals create a new centralised database that would contain information about millions of third-country nationals, including their biometric data. Due to its scale and the nature of the data to be stored in this database, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights. It is therefore essential to build strong legal, technical and organizational safeguards. Special vigilance is also required both as regards the purposes of the database as well as its conditions and modalities of use.

In this context, the EDPS stresses the importance of further clarifying the extent of the problem of identity fraud among third-country nationals, in order to ensure that the measure proposed is appropriate and proportionate. The possibility to consult the centralized database to facilitate identity checks on the territory of the Member States should be framed more narrowly.

The EDPS understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, facilitating the access by law enforcement authorities to non-law enforcement systems (i.e. to information obtained by authorities for purposes other than law enforcement), even to a limited extent, is far from insignificant from a fundamental rights perspective. Routine access would indeed represent a serious violation of the principle of purpose limitation. The EDPS therefore calls for the maintenance of genuine safeguards to preserve fundamental rights of third country nationals.

Finally the EDPS would like to stress that both in legal and technical terms, the Proposals add another layer of complexity to the existing systems, as well as those that are still in the pipeline with precise implications that are difficult to assess at this stage. This complexity will have implications not only for data protection, but also for governance and supervision of the systems. The precise implications for the rights and freedoms which are at the core of the EU project are difficult to fully assess at this stage. For these reasons, the EDPS calls for a wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context.

1. INTRODUCTION

1.1. Background

1. In April 2016, the Commission adopted a Communication *Stronger and Smarter Information Systems for Borders and Security* ([1]) initiating a discussion on how information systems in the European Union could better enhance border management and internal security.

2. In June 2016, as a follow-up of the Communication, the Commission set up a high-level expert group on information systems and interoperability ('HLEG'). The HLEG was tasked to address legal, technical and operational challenges to achieving interoperability between central EU systems for borders and security ([2]).

3. The HLEG presented recommendations first in its interim report of December 2016 ([3]), and later in its final report of May 2017 ([4]). The EDPS was invited to take part in the works of the HLEG and issued a statement on the concept of interoperability in the field of migration, asylum and security which is included in the final report of the HLEG.

4. Building on the Communication of 2016 and the recommendations of the HLEG, the Commission proposed a new approach where all centralised EU information systems for security, border and migration management would be interoperable ([5]). The Commission announced its intention to work towards creating a European search portal, a shared biometric matching service and a common identity repository.

5. On 8 June 2017, the Council welcomed the Commission's view and the proposed way forward to achieve the interoperability of information systems by 2020 ([6]). On 27 July 2017, the Commission launched a public consultation on the interoperability of EU information systems for borders and security ([7]). The consultation was accompanied by an inception impact assessment.

6. On 17 November 2017, as an additional contribution, the EDPS issued a reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice ([8]). In this paper he recognised that interoperability, when implemented in a well thought-out-manner and in compliance with the core requirements of necessity and proportionality, may be a useful tool to address legitimate needs of competent authorities using large scale information systems including improve information sharing.

7. On 12 December 2017, the Commission published two legislative proposals ('the Proposals') 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, hereinafter 'Proposal on borders and visa'.

— 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) hereinafter 'Proposal police and judicial cooperation, asylum and migration'.

([1]) Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security, 6.4.2017, COM (2016) 205 final.
([2]) Idem, p. 15.
([3]) Interim report by the chair of the high-level expert group on information systems and interoperability set up by the European Commission, Interim report by the chair of the high-level expert group, December 2016, available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.
([4]) Final report of the high-level expert group on information systems and interoperability set up by the European Commission, 11 May 2017; available at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.
([5]) Communication of 16.5.2017 from the Commission to the European Parliament, the European Council and the Council, Seventh progress report towards an effective and genuine Security Union, COM(2017) 261 final.
([6]) Council conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems, 8 June 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/en/pdf.
([7]) The public consultation and the impact assessment are available at: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.
([8]) https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.

1.2. **Objectives of the Proposals**

8. The Proposals aim in general at improving the management of the Schengen external borders and at contributing to the internal security of the European Union. To this end, they establish a framework to ensure the interoperability between existing and future EU large scale information systems in the areas of border checks, asylum and immigration, police cooperation and judicial cooperation in criminal matters.

9. The interoperability components established by the Proposals would cover:

— Three existing systems: the Schengen Information System (SIS), the Eurodac system and the Visa Information System (VIS);

— Three proposed systems that are still in preparation or development:

— one that has recently been agreed on by the EU legislators and needs to be developed: the Entry/Exit System (EES) ([1]) and,

— two that are still under negotiations: the proposed European Travel Information and Authorisation System (ETIAS) ([2]), and the proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN) ([3]);

— the Interpol's Stolen and Lost Travel Documents (SLTD) database and

— Europol data ([4]).

10. The interoperability between these systems consists of four components:

— A European search portal ('ESP'),

— A shared biometric matching service ('shared BMS'),

— A common identity repository ('CIR') and,

— A multiple identity detector ('MID').

11. The ESP would work as a message broker. Its purpose is to provide a simple interface that would provide fast query results in a transparent way. It would enable the simultaneous query of the different systems using identity data (both biographical and biometric). In other words, the end-user would be able to carry out a single search and receive results from all the systems he/she is authorised to access rather than searching each system individually.

12. The shared BMS would be a technical tool to facilitate the identification of an individual who may be registered in different databases. It would store templates of the biometric data (fingerprints and facial images) contained in the EU centralised information systems (i.e. the SIS, the Eurodac system, the EES, the VIS and the ECRIS-TCN). It would enable on the one hand, to simultaneously search biometric data stored in the different systems and on the other hand, to compare these data.

13. The CIR would facilitate the identification of persons including on the territory of Member States and also help streamlining the access by law enforcement authorities to non-law information systems. The CIR would store biographical and biometric data recorded in the VIS, the ECRIS-TCN, the EES, the Eurodac system and the ETIAS). It would store the data — logically separated — according to the system from which the data was originated.

([1]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

([2]) Proposal for a Regulation of the European parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final, 16.11.2016.

([3]) Proposal for a Regulation of the European Parliament and of the Council establishing a centralized system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, COM(2017) 344 final, 29.6.2017.

([4]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

14. The MID would be a tool that would allow to link identities within the CIR and the SIS and would store links between records. It would store links providing information when one or more definite or possible match(es) is(are) detected and/or when a fraud identity is used. It would check whether queried or input data exists in more than one of the systems to detect multiple identities (e.g. same biometric data linked to different biographical data or same/similar biographical data linked to different biometric data). The MID would show the biographical identity records that have a link in the different systems.

15. Through the four interoperability components, the Proposals aim at:

— providing authorised users with fast, seamless, systematic and controlled access to relevant information systems,

— facilitating identity checks of third country nationals on the territory of Member States,

— detect multiple identities linked to the same set of data and,

— streamline the access of law enforcement authorities to non-law enforcement information systems.

16. In addition, the Proposals would establish a central repository for reporting and statistics ('CRRS'), the Universal Message Format ('UMF') and would introduce automated data quality control mechanisms.

17. The publication of two legislative proposals instead of one results from the need to respect the distinction between systems that concern:

— the Schengen *acquis* regarding borders and visas (i.e. the VIS, the EES, the ETIAS and the SIS as regulated by Regulation (EC) No 1987/2006),

— the Schengen *acquis* on police cooperation or that are not related to the Schengen *acquis* (the Eurodac system, the ECRIS-TCN and the SIS as regulated by Council Decision 2007/533/JHA).

18. The two Proposals are 'sister proposals' that have to be read together. The numbering of the Articles is mainly similar in both proposals as is their content. Therefore, unless otherwise specified, when we mention a specific Article, this Article is referring to the one of both proposals.

5. **CONCLUSIONS**

142. The EDPS recognises that interoperability, when implemented in a well thought-out manner and in compliance with the core requirements of necessity and proportionality, may be a useful tool to address legitimate needs of competent authorities using large scale information systems including improve information sharing.

143. He stresses that interoperability is not primarily a technical choice, it is first and foremost a political choice to be made, with significant legal and societal implications in the years to come. Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters), as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'. For these reasons, the EDPS calls for a wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context.

144. Although the Proposals as presented could give the impression of interoperability as the final component of already fully functioning information systems (or at least systems the legal founding acts of which are already 'stable' and in the final stages of the legislative process), the EDPS wishes to recall that this is not the case. In reality, three of the six EU information systems the Proposals seek to interconnect do not exist at the moment (ETIAS, ECRIS-TCN and EES), two are currently under revision (SIS and Eurodac) and one is to be revised later this year (VIS). Assessing the precise implications for privacy and data protection of a very complex system with so many 'moving parts' is all but impossible. The EDPS recalls the importance to ensure consistency between the legal texts already under negotiation (or upcoming) and the Proposals in order to ensure a unified legal, organizational and technical environment for all data processing activities within the Union. In this context, he would like to stress that this Opinion is without prejudice to further interventions that may follow as the various interlinked legal instruments progress through the legislative process.

145. The EDPS notes that while interoperability might have been envisaged initially as a tool to only facilitate the use of the systems, the Proposals introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks and streamline access by law enforcement authorities to non-law information systems.

146. As already stressed in his reflection paper, the EDPS stresses the importance of first further clarifying the extent of the problem of identity fraud among third-country nationals so as to ensure that the measure proposed is appropriate and proportionate.

147. As regards the use of the data stored in the various systems to facilitate identity checks on the territories of the Member States, the EDPS highlights that the purposes of such use, i.e. combating irregular migration and contributing to a high level of security are formulated too broadly and should be 'strictly restricted' and 'precisely defined' in the Proposals so as to comply with the case law of the Court of Justice of the European Union. He considers in particular that access to the CIR to establish the identity of a third country national for purposes of ensuring a high level of security should only be allowed where access for the same purposes to similar national databases (e.g. register of nationals/residents etc.) exist and under the same conditions. He recommends to make this clear in the Proposals. Otherwise, the Proposals would appear to establish a presumption that third country nationals constitute by definition a security threat. He also recommends to ensure that access to the data to identify a person during an identity check would be allowed:

— in principle, in the presence of the person and,

— where he or she is unable to cooperate and does not have document establishing his/her identity or,

— refuses to cooperate or,

where there are justified or well-founded grounds to believe that documents presented are false or that the person is not telling the truth about his/her identity.

148. The EDPS understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts as other serious crimes. However, removing genuine safeguards introduced to preserve fundamental rights mainly in the interest of speeding up a procedure would not be acceptable. He therefore recommends to add in Article 22(1) of the Proposals the conditions related to the existence of reasonable grounds, the carrying out of a prior search in national databases and the launching of a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA, prior to any search in the common repository for identity. In addition, he considers that the compliance with the conditions of access to even limited information such as a hit/no hit should always be verified, independently of further access to the data stored in the system that triggered the hit.

149. The EDPS considers that the necessity and the proportionality of the use of the data stored in the ECRIS-TCN to detect multiple identities and to facilitate identity checks should be more clearly demonstrated, and require clarification also with regard to its compatibility with the purpose limitation principle. He therefore recommends to ensure in the Proposals that the data stored in the ECRIS- TCN could be accessed and used solely for the purposes of the ECRIS TCN as defined in its legal instrument.

150. The EDPS welcomes that the Proposals aim at the creation of a harmonized technical environment of systems that will work together to provide fast, seamless, controlled, and systematic access to the information the various stakeholders need to perform their tasks. He recalls that the fundamental data protection principles should be taken into account during all stages of the implementation of the Proposals and consequently recommends to include in the Proposals the obligation for eu-LISA and the Member States to follow the principles of data protection by design and by default.

151. Beyond the general comments and key issues identified above, the EDPS has additional recommendations related to the following aspects of the Proposals:

— the functionality of the ESP, the shared BMS, the CIR and the MID,

— the data retention periods in the CIR and the MID,

— the manual verification of links,

— the central repository for reporting and statistics,

— the division of roles and responsibility between eu-LISA and the Member States,

— the security of the interoperability components,

— the data subjects' rights,

— the access by eu-LISA staff

— the transitional period,

— the logs and

— the role of the national supervisory authorities and the EDPS.

152. The EDPS remains available to provide further advice on the Proposals, also in relation to any delegated or implementing act adopted pursuant to the proposed Regulations which might have an impact on the processing of personal data.

Brussels, 19 March 2018.

Giovanni BUTTARELLI

European Data Protection Supervisor