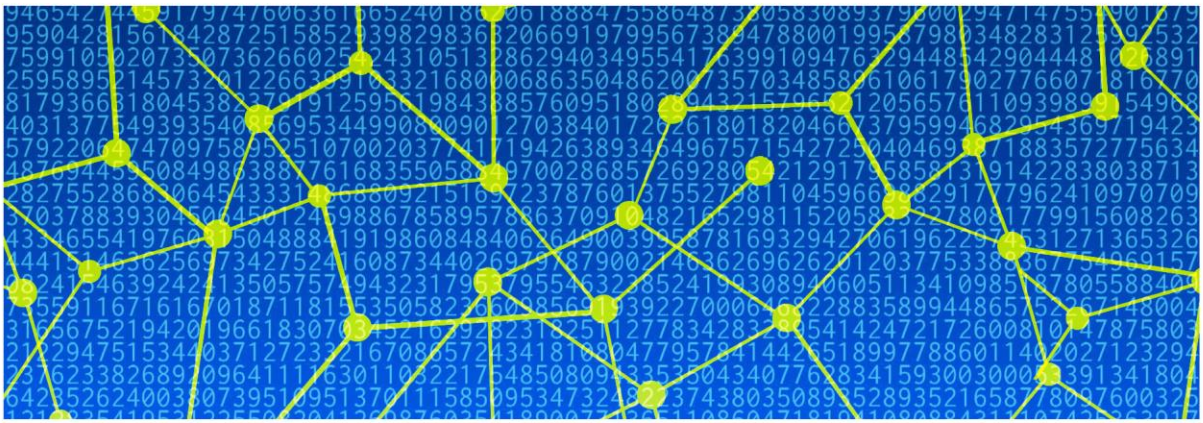

EUROPEAN DATA PROTECTION SUPERVISOR

Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice

EDPS

17 November 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

The initiative of this Reflection Paper is to contribute to the preparatory work on the forthcoming legislative proposal on interoperability between EU large scale information systems for borders management and security. It relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking -in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that compliance with data protection requirements is key to an effective and efficient information management for borders management and security.

Executive Summary

In principle, interoperability aims at developing effective and efficient information sharing to ensure that competent authorities at national and EU level get the right information at the right time. Interoperability, when implemented in a well thought-out manner, may help address some needs of competent authorities using large scale information systems and help reduce the overall cost of operating such systems. Interoperability may also be in the interest of data protection. For instance, interconnecting information systems which have closely related purposes and that in addition contain some identical data could help avoiding that the same or similar data are stored, validated and updated many times, once in each system.

The terrorist attacks that occurred on the EU territory have heightened security concerns. In addition, in the last years, EU has been confronted with a massive influx of refugees and migrants. These events have prompted the EU Commission to consider several initiatives, including the interoperability of the EU large scale information systems created for migration, border management and/or police cooperation.

While we note that the Commission might have envisaged interoperability as a tool to only facilitate the use of systems, we understand that the Commission may consider to extend it to new possibilities of exchanging or cross-matching data.

Since introducing interoperability is likely to imply new (or changed) personal data processing, such changes would require a clear basis in legislation in full compliance with the EU Charter of Fundamental Rights. In particular, any new or modified data processing would need to be clearly defined in the relevant legal instrument and be equally necessary and proportionate in relation to its clearly stated objectives.

Compliance with EU data protection rules goes beyond the principles of data protection by design/default, the obligation to apply security measures, etc. and requires that necessity and proportionality of processing are first established.

We therefore look forward to the European Commission forthcoming legislative proposal that should clearly define the problems interoperability aims to solve. It should also clearly set out for which specific purposes what categories of personal data would be processed in the context of its future initiatives on interoperability. This will allow a proper debate on interoperability from the fundamental rights perspective. Performing a full assessment of the impact of interoperability on fundamental rights to privacy and data protection will be fundamental once more details about the planned initiative are known. The forthcoming legislative proposal could in this sense represent an opportunity to be seized for designing a more coherent and consistent framework.

TABLE OF CONTENTS

1 Ongoing initiatives in the context of "interoperability" of large-scale IT systems

1 The terrorist attacks that occurred on the EU territory have heightened security concerns. In addition, the EU has in the past few years been confronted with a massive influx of refugees and migrants. These events have prompted the EU Commission to consider several initiatives which include the creation of new large-scale EU information systems[1], the modification of existing ones[2] as well as the interoperability of all these systems.

2 In its Communication of 6 April 2016 "*Stronger and Smarter Information Systems for Borders and Security"* ("Communication of 2016")[3], the Commission emphasized the need to improve the interoperability of information systems; it also presented ideas on how information systems could be developed in the future. The Commission set up a high-level expert group on information systems and interoperability ("HLEG"). The HLEG was tasked to address "the legal, technical and operational aspects of the different options to achieve the interoperability of the information systems, including the necessity, technical feasibility and proportionality of available options and their data protection implications"[4].

3 The HLEG presented recommendations on strengthening and developing the EU's information systems and interoperability first in its interim report of December 2016[5], and later in its final report of May 2017[6]. The EDPS was invited to take part in the works of the HLEG. He 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 In its seventh Progress report towards an effective and genuine security union[7], the Commission set out a new approach to the management of data for borders and security in line with the Communication of 2016 and the recommendations of the HLEG. Under this approach, all centralised EU information systems for security, border and migration management should be interoperable so that:

- the systems can be searched simultaneously using a European search portal, possibly with more streamlined rules for law enforcement access;
- the systems use one shared biometric matching service to enable searches across different information systems holding biometric data, possibly with hit/no-hit flags indicating the connection with related biometric data found in another system;
- the systems share a common identity repository with alphanumeric identity data to detect if a person is registered under multiple identities in different databases.

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. It invited the Commission to pursue the work on three dimensions of interoperability (i.e. the European search portal, the biometric matching service and a common identity repository)[8].

On 27 July 2017, the Commission launched a public consultation on the interoperability of EU information systems for borders and security[9]. The consultation was accompanied by an inception impact assessment. In its indicative planning of 2 October[10], the Commission mentions the date of 12 December for the adoption of the legislative proposal on interoperability.

6 Looking forward to the forthcoming legislative proposal, this reflection paper is our additional contribution. It will be followed by a formal Opinion of the EDPS under Article 28(2) of Regulation 45/2001.

2 The concept of interoperability

7 Interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged. Although interoperability is often considered as a merely technical concept, we consider that in the present context it cannot be disconnected from the questions whether the data exchange is necessary, politically desirable or legally possible. In other words, although interoperability of the information systems will ultimately be implemented through technical means, it must be subject to political debate on its purposes and future scope.

8 We observe that making exchange of data technically feasible becomes, in many cases, a powerful drive for exchange these data. One can safely assume that technical means will be used, once they are made available; in other words, the risk is that in such case the means justify the end. To allow a proper debate about the risks and advantages of interoperability, it is fundamental to give it an unambiguous and clear meaning.

9 We note that interoperability may work at different levels, from a mere communication infrastructure between two systems to the ability of these systems to both exchange and use the information that has been exchanged. We recognise that, when implemented in a well thought-out manner, interoperability may help address some needs of competent authorities using large scale information systems as well as reduce the overall cost of operating such systems. Interoperability may also provide some benefits in terms of data protection. For instance, interconnecting information systems which have closely related purposes and that in addition contain some identical data could help avoiding that the same data are stored twice, once in each system[11].

10 Interoperability would in principle aim to render currently applicable rules more effective and efficient. For instance, the European search portal envisaged by the Commission would enable competent authorities to query several systems simultaneously instead of having to query each system separately. When such queries are performed by authorised competent authorities with full respect of their access rights and in line with the respective purposes of each system as defined in its legal bases, there would not be any fundamental data protection issues. A user would access only the information they are allowed to access and exclusively for the specific purpose(s) of the system in question.

11 However, while we note that the Commission might have envisaged interoperability as a tool to only facilitate the use of systems, we understand that the Commission now may aim to extend it to new possibilities of exchanging or cross-matching data. For instance, the inception impact assessment refers to the use of a shared biometric matching service ('the BMS') to enable matching of biometric data held across the various systems. Similarly, a 'common identity repository' would bring together alphanumeric data (such as names and dates of birth) that have been stored in the various systems for border management and security. The combined use of the shared BMS and the common identity repository would enable single identification using alphanumeric and/or biometric data to detect multiple

identities. Interoperability thus implies new data processing that are not covered by existing legal bases and their impact on the fundamental rights to privacy and data protection needs to be carefully assessed.

3 Interoperability from a data protection perspective

3.1 Personal data "must be processed fairly for specified purposes"

12 We are of the opinion that interoperability should not be an end in and of itself, but should always serve a genuine public interest objective. The inception impact assessment first refers to the general objective of "developing stronger and smarter information systems for borders and security". It then mentions the following specific objectives:

- ensuring that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast and seamless access to all information that they need to perform their tasks;
- facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems where necessary for the prevention, investigation, detection or prosecution of criminal offences;
- providing a solution to detect and combat identity fraud[12].

13 In this context, it is important to stress that general policy objectives such as those enlisted in the inception impact assessment do not necessarily equal a public interest objective in accordance with the law, as for example according to Article 52(1) of the Charter, and the purposes of data processing under data protection law. The mentioned objectives appear to focus on what interoperability would achieve in the technical sense. However, the envisaged data processing, the public interest and their specific purpose(s) are not explained. Instead, the inception impact assessment seems to equate the *processing* that interoperability would facilitate or permit (e.g. the consultation, access, use, retrieval, etc. of the data) with the *purpose*s of processing.

14 We encourage the Commission to clearly describe the specific purposes of the envisaged data processing. Objectives such as "ensuring fast and seamless access to databases" might be a useful means to an end in policy terms. However, they are not specific enough for the purposes of data protection law since they are not linked to specific processing of defined categories of personal data. Consequently, they may not allow individuals to understand which of their personal data are processed for what precise purposes, or to understand the consequences of such processing.

15 It is important to understand that purpose specification is a fundamental prerequisite for the application of many other principles of data protection. Only clear and specific purposes will allow to determine the relevant data to be collected, the applicable retention periods, and many other key aspects of how personal data will be processed for the chosen purpose(s). The description of the public interest objective may not meet the requirement of the purpose specification, in particular when the public interest may have different aspects[13]. Therefore we recommend that the forthcoming legislative proposal clearly set out the precise purposes of the various data processing envisaged.

3.2 Clarifying the needs for interoperability

16 A clear description of the purposes of the proposed data processing will also be essential to assessing their necessity and proportionality. Such purposes must be sufficiently detailed not only so as to allow an objective assessment of whether the proposed collection and use complies with the law, but also to establish which safeguards should apply. We refer to the "Necessity toolkit" for easy-to use advice to EU legislator on how to assess compliance with regard to Articles 7, 8 and 52(1) of the Charter. In particular, the assessment of necessity and proportionality requires the legislator to precisely identify what the proposed measure entails in terms of personal data processing and what the objective(s) and the concrete purpose(s) of the measure is. The problems the measure addresses should also be sufficiently and clearly described and be accompanied by objectives evidence of their existence. Finally, it should be demonstrated that no other means which would be less invasive are available to achieve the envisaged purpose(s)[14].

17 We note that the inception impact assessment refers to four main shortcomings highlighted in the Communication of 2016: *i.e.*
- the sub-optimal functionalities of existing information systems;
- gaps in the EU architecture of data management;
- a complex landscape of differently governed information systems and
- a fragmented architecture of data management for border control and security.

18 Interoperability between systems is then mentioned as fundamental to addressing the above shortcomings, especially as regards:
- the lack of complete and accurate data;
- the lack of fast and seamless access to all information;
- the conditions law enforcement have to comply with to access non law enforcement databases and
- identify fraud.

19 However, while the inception impact assessment identifies certain problems, it does not describe in detail what the precise issues are. It is often not clear whether the underlying problem is of a legal nature, a technical one or both. For example, what is meant exactly by "the lack of a fast and seamless access to all information"? Is it a legal issue (i.e. the current legal basis does not allow a user to access certain data) or a technical one (e.g. the response time of the system is too long), or perhaps both? Depending on how the problem is defined, the appropriate solution to address it might differ, in particular in terms of data processing. Without a clear and sufficiently detailed description of the problems and needs, it is difficult to make sure that the proposed policy options (i.e. the establishment of a European search portal, a shared BMS or a common repository) are appropriate, proportionate and fully address the identified needs.

20 In other words, only a clear description of the identified problems in view of the objectives pursued will allow the EU legislator to determine the most appropriate legal and technical solutions, in compliance with data protection law. Technology should always come in support of policies and user needs, not the other way around. What is technically feasible might not necessarily be legally justifiable or ethically desirable. As highlighted in the preamble to the General Data Protection Regulation, "the processing of personal data should be designed to serve mankind"[15].

3.3 Purpose limitation with regard to migration, asylum, police and judicial cooperation

21 We would like to stress the importance of considering interoperability of information systems also taking into account the policy context in which the existing information systems had been built. Interoperability as envisaged by the Commission would impact instruments set up to support policies in the field of (i) border checks, asylum and immigration, as well as (ii) police cooperation and (iii) judicial cooperation. There is an increasing trend in EU policy-making to associate migration management and security purposes. We see this trend in the context of granting access to existing systems for law enforcement purposes[16], building a new information system[17], or extending the competences of an existing body[18]. We are concerned that repeatedly referring to migration, internal security and fight against terrorism almost interchangeably brings the risk of blurring the boundaries between migration management and fight against terrorism. It may even contribute to creating assimilation between terrorists and foreigners.

22 While the existing systems have been developed with separate application of European migration and law enforcement policies in mind, we recognise that synergies might exist between migration and police cooperation policies and objectives. Nevertheless, it should be kept in mind that migration on the one hand, and police cooperation on the other hand, remain two different areas of public policy and objectives of public interest based on distinct legal bases in the TFEU and pursuing specific objectives that need to be clearly distinguished. This may have an impact on the assessment of compatibility of purposes of data processing that the Commission needs to take into consideration in the context of the forthcoming legislative proposal.

3.4 The proposed options for interoperability

23 We would like to already draw the attention of the EU legislator to some data protection issues that may arise in relation to some of the specific solutions that are currently under discussion, assuming that:

- the forthcoming legislative proposal will clearly describe the identified purposes, objectives and needs as a result of encountered problems and,
- sufficient information will be provided to assess the necessity and proportionality of the chosen solutions[19].

These issues concern in particular the conditions of access to the databases, the use of existing databases for new/additional purposes, and data security.

New (modalities of) access

24 The inception impact assessment mentions that in cases where end users would not have access to certain data in the central systems, the European search portal (through alphanumeric data) and the shared biometric service (through biometric data) would provide access on a “hit/no hit” basis, i.e. indicating the mere presence of relevant data in underlying systems, without however revealing that data.

25 Depending on the objective(s) of such new functionality, it could be considered as:
- a new instance of personal data processing, i.e. *a new access*: the authority is not allowed to access the data recorded in a specific system but would know whether that system contains information about a specific individual or not;
- a change in *conditions applicable to data processing* (in this instance: conditions of access to personal data): the authority is already allowed to access the data but subject to certain conditions (which from fundamental rights perspective may function as *safeguards*). Under the proposed "hit/no hit" approach, an authority would have direct access to a database that would allow it to verify whether or not the database contains information about a specific individual. However, it would only get a yes ("hit") or no ("no hit") answer. In case of a positive answer ("hit"), the authority would have to fulfil specific condition(s) to access further information (e.g. an authorisation from an independent authority).

26 In case of a *new access* as described above, it is important to clarify that the existence (or lack) of a "hit" is personal data even with the absolute minimum of information (e.g. known or unknown in a given system) since it amounts to information related to a person (e.g. the person in question is or is not subject to an alert in the Schengen Information System). Consequently, a user who is not allowed to access data stored in a specific system is similarly not allowed to get access to "hit/no hit" information, since even this limited information constitutes personal data. Besides, we wonder what would be the usefulness of such a feature, given that knowing that information exists ("hit") without being authorised to access the full range of data would normally not be useful in the decision making process and it might be contrary to the data protection principle of data quality (i.e. only the personal data which are necessary for the stated purpose may be processed).

27 Regarding the "hit/no hit" approach as a *condition for access*, the EDPS understands that the aim of such an approach could be to provide some safeguards (i.e. limited access) that would replace one or several conditions with which law enforcement authorities have to comply today when accessing non-law enforcement databases.

28 Currently, a law enforcement authority willing to access non-law enforcement databases has to comply with several conditions (e.g. access needed in a specific case, substantiated suspicion, prior check of national databases, etc.). This also includes the prior authorisation by another authority acting independently and being responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences. Before granting authorisation, such an authority verifies whether all the conditions of access provided for in the legal basis of the respective information system are complied with.

29 The HLEG report suggests that, in order to identify whether a large-scale system contains (or not) information about an individual, law enforcement authorities should be allowed to access non-law enforcement information systems without prior authorisation. For other purposes (such as for instance reconstructing the travel history of a known suspect in the context of a specific investigation) prior authorisation would remain mandatory.

30 It is worth pointing out in this context that EU large scale information systems - such as the Visa Information System or Eurodac - have been put in place for migration and asylum purposes. The possibility for law enforcement authorities to access these databases has been added at a later stage, and only subject to specific conditions (guarantees) to limit undue impact on individuals. Therefore, any potential relaxation of such existing conditions

would need to be specifically justified and would require a thorough and comprehensive analysis of all remaining and/or new safeguards to assess whether such relaxation would be necessary and proportionate. In particular, in order to preserve a sufficiently high level of protection against possible abuse, reduced safeguards of *ex ante* controls should at the very least be accompanied by strengthening *ex post* controls.

New uses of data

31 The inception impact assessment mentions that the shared biometric matching service ("BMS") would enable the matching of biometric data held in the various databases, while the common identity repository would bring together alphanumeric data (such as names and dates of birth) that have been stored in the various information systems for border management and security. The combined use of the shared BMS and the common identity repository would allow to detect multiple identities linked to the same biometric data present in the various large-scale systems and would thus help combat identity fraud.

32 It should be kept in mind that the use of unique identifiers, combined with technical possibilities to collect all available information on the individuals from other information systems, would amount to a new processing of personal data that must be adequately and sufficiently justified (see sections 3.1 and 3.2).

33 In addition, the information systems that would feed the common identity repository had been built for purposes other than combating identity fraud which would constitute a new purpose of data processing. In this context, we see a risk of "function creep" (i.e. a widening of the use of a system or a database beyond the purpose(s) for which it was originally intended). As with any initiative that would potentially allow for further uses of data or systems beyond what was originally foreseen by law, we would advise a cautious approach. The argument that, since the data is already collected, they can just as well be used for other purposes cannot be uncritically accepted, since such new processing might have a bigger impact on individuals.

34 Finally, we would like to use this opportunity to clarify the principle of data minimisation which is often misunderstood. For example, the Communication of 2016 mentions that the storage of the same data in different information systems is contrary to the data minimisation principle. The inception impact assessment further specifies that a common identity repository would help improve efficiency by avoiding duplication of data. However, avoiding duplication of data will not *per se* ensure data minimisation. Under data protection law, the data minimisation principle requires first and foremost that the collection and processing of data is limited to those adequate, relevant and necessary for the envisaged purposes[20]. That means in practice that sharing data between databases which process the same data will not necessarily be sufficient to implement the principle of data minimisation.

New security challenges

35 We wish to draw attention on the fact that interoperability - as conceived so far by the Commission - would introduce a fundamental change in the current architecture of large-scale IT systems: a shift from a closed environment to a shared environment with connectivity between the various systems. This would bring about new security risks. To take the case of the European search portal as an example, such risks would arise for

instance from the fact that an attacker would have to compromise only one single point of access (instead of multiple point of access, i.e. one for each information systems) to get access to several large-scale information systems.

36 It is therefore of paramount importance to properly analyse the information security consequences of the various options proposed to achieve interoperability. A comprehensive information security risk management following Article 22 of Regulation (EC) No 45/2001 and EDPS guidance appears as necessary before implementing any change that may affect the security of all systems[21].

4 Conclusions

37 We support interoperability, when implemented in a well thought-out manner and in compliance with core requirements of necessity and proportionality. Interoperability may be then a useful tool to address legitimate needs of competent authorities using EU large scale information systems including improve information sharing.

38 Although interoperability is often considered as a merely technical concept, it cannot be disconnected, in the present context, from the questions whether the data exchange is genuinely necessary, politically desirable or legally justifiable.

39 From a fundamental rights perspective, we consider that the Commission might have envisaged interoperability as a tool to only facilitate the use of systems and to only render currently applicable rules more effective and efficient. However, we understand that the Commission may consider to extend it to new possibilities of exchanging or cross-matching data. This would imply new data processing that are not covered by existing legal instruments. Their impact on the fundamental rights to privacy and data protection would need to be carefully assessed.

40 It is important to keep in mind that compliance with EU data protection rules goes beyond the principles of data protection by design/default, the obligation to apply security measures, etc. and requires that necessity and proportionality of processing are first established.

41 In particular, the problems interoperability aims to solve should be clearly identified in the forthcoming legislative proposal so as to allow a proper debate from the fundamental rights perspective. We note that the Commission identifies certain problems, but does not describe in detail what the precise issues are. It is often not clear whether the underlying problem is of a legal nature, a technical one or both. Depending on the problem, the appropriate solution to address it might differ, in particular in terms of data processing. The proposal should also clearly state for which specific purposes what categories of personal data would be processed.

42 Consequently, we consider that performing a full assessment of the impact of interoperability on fundamental rights to privacy and data protection will be fundamental once more details about the planned initiative are known. The forthcoming legislative proposal could in this sense represent an opportunity to be seized for designing a more coherent and consistent framework.

Brussels, 17 November 2017

Giovanni BUTTARELLI

Notes

[1] See for instance the Proposal for a Regulation of the European Parliament and of the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM (2016) 194 final; 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.

[2] See for instance the SIS legislative package consisting of (i) the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM(2016) 882 final; (ii) the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM(2016) 883 final and (iii) the Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third country nationals, COM(2016) 881 final. See also the Proposal for a Regulation of the European Parliament and of the Council on amending Regulation (EU) No 603/2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person, for identifying an illegally staying third country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2016)272 final.

[3] 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.

[4] Idem, p. 15.

[5] 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.

[6] 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

[7] Communication of 16.05.2017 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.

[8] 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.

[9]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.

[10] Tentative agendas for forthcoming Commission meetings, http://ec.europa.eu/transparency/regdoc/rep/2/2017/EN/SEC-2017-415-F1-EN-MAIN-PART-1.PDF.

[11] See EDPS opinion 6/2016 on the second EU smart borders package, point III.3.d) p. 15 https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf.

[12] Inception impact assessment, p.2.

[13] See 'Step 3' of the "necessity toolkit" issued by the EDPS on 11 April 2017, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[14] See the "necessity toolkit" issued by the EDPS on 11 April 2017, which aims to better equip EU legislators responsible for preparing and scrutinising measures which involve the processing of personal data and which might interfere with the rights to privacy, data protection and other rights and freedoms laid down in the Charter of Fundamental Rights of the EU; available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[15] 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), JOCE, 4.5.2016, L 119/1.

[16] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, O.J. L 218, 13.08.2008, p.

129; Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), O.J. L 180, 29.06.2013, p.1.

[17] See for instance the Proposal for a Regulation of the European Parliament and of the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM (2016) 194 final. See also the 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.

[18]Proposal for a Regulation on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC (COM(2015) 671 final).

[19]See the "necessity toolkit" issued by the EDPS on 11 April 2017, which aims to better equip EU legislators responsible for preparing and scrutinising measures which involve the processing of personal data and which might interfere with the rights to privacy, data protection and other rights and freedoms laid down in the Charter of Fundamental Rights of the EU; available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[20] Under Article 5(1)(c) of the General Data Protection Regulation, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

[21]Guidance on Security measures for Personal Data Processing, Article 22 of Regulation 45/2001, https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf.