EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems

EDPS

16 April 2018

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.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and to foster accountable policymaking in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. It follows the reflection paper the EDPS issued on 17 November 2017. The EDPS considers that compliance with data protection requirements is key to the success in making the EU large-scale information systems in the Area of Freedom, Security and Justice interoperable.

Executive Summary

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.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and to 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)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[4], and to 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[5],

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1.1 Background

1 In April 2016, the Commission adopted a Communication *Stronger and Smarter Information Systems for Borders and Security*[6] 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.[7]

3 The HLEG presented recommendations first in its interim report of December 2016[8], and later in its final report of May 2017[9]. 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.[10] 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.[11] On 27 July 2017, the Commission launched a public consultation on the interoperability of EU information systems for borders and security[12]. 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.[13] 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'.

1.2 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)[14] and,
  - two that are still under negotiations: the proposed European Travel Information and Authorisation System (ETIAS)[15], and the proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN)[16];

- the Interpol's Stolen and Lost Travel Documents (SLTD) database and
- Europol data.[17]

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.

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.

2. General comments

19 Today's pressing security and border management challenges require smarter use of the information already available to the authorities. Interoperability, when implemented in a well-thought manner, may contribute to the development of effective and efficient information sharing. In this context, the EDPS has supported the Commission's initiative starting the reflection on an overall strategic vision on how to make the management and use of data more effective and efficient in full compliance with data protection[18]. He has recognised that interoperability, when developed in full compliance with fundamental rights, may be a useful tool to address legitimate needs of competent authorities using large scale information systems.

20 The EDPS observed in the recent years an increasing trend of addressing security and migration management purposes jointly. Examples of this trend include granting access to existing migration information systems for law enforcement purposes[19], creating EU information systems with dual purposes[20] or the extension of mandates of EU agencies.[21] By creating interoperability between migration, police cooperation but also judicial cooperation tools, the Proposals are part of this trend. As already stressed in his reflection paper, the EDPS is 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 crime and terrorism. It may even contribute to creating assimilation between terrorists, criminals and foreigners.

21 Furthermore, he notes that while 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).

22 Assessing the precise implications for privacy and data protection of a system with so many "moving parts" is all but impossible. 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. Interoperability implemented this way leads to more complexity rather than simplification. While the EDPS understands the reasons behind the proposals,

adding more complexity may undermine the very objective as laid down in Article 2(2)(e) of the Proposals which is the strengthening and simplifying and making more uniform the data security and data protections that govern the respective EU information systems.

23 This complexity will have implications not only for data protection, but also for governance and supervision of the systems. In this context, the EDPS recalls that EU large-scale information systems in the area of Freedom, Security and Justice have a huge impact on the fundamental rights of the individuals including their rights to data protection and thus require efficient and strong independent supervision. As a result, he stresses the need to provide Data Protection Authorities including the EDPS with the necessary additional financial and human resources to enable them to duly perform their supervisory role.

24 The Proposals as presented give the impression of interoperability as the final component of already fully functioning information systems (or at least for which the legal founding instruments are stable according to the legislative process). As mentioned above, this is not the case; from a standpoint of consistency and with respect to the democratic process, it would have been preferable to present the Proposals after the adoption of the various pending legal instruments or, at least, to present all the relevant legislative proposals together at the same time. It is important to ensure consistency between the legal texts already under negotiation (or upcoming) and the Proposals so there is a unified legal, organizational and technical environment for all data processing activities within the Union. In this context, the EDPS 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.

25 The EDPS recognises that, nowadays even more than ever, there is a need to better share information and use more efficiently the EU large scale information systems to manage migratory challenges on the one hand and to tackle terrorist and crime-related issues on the other hand. However, the need for better exploitation of the data should never lead to the violation of the fundamental right to data protection. Interoperability is not primarily a technical choice, it is in particular a political choice to be made. 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.

26 Finally, the EDPS would like to recall that the protection of the fundamental rights including the rights to privacy and data protection as enshrined in the EU Charter of fundamental rights is not limited to EU nationals. EU and Member States are bound by it when applying EU law to individual whether or not he/she is a EU citizen, a third country national, a migrant (irregular or not), or an asylum seeker. The Charter must be the compass for all EU policies and laws. The EDPS stands ready to assist the EU legislator in ensuring that it does.

3. Main recommendations

3.1 Introduction

27 As already stressed in his reflection paper, the EDPS is of the opinion that interoperability should not be an end in itself but should always serve a genuine public interest objective. He therefore welcomes that the Proposals list the objectives of general interest they pursue as well as the more specific objectives interoperability aims at achieving.

28 He is of the opinion that interoperability as set out in the Proposals is more than the sum of its parts as its components ultimately contribute together to establish a central database of third country nationals, in particular a central biometric register of third country nationals. A central database - in contrast to decentralised databases - implicitly increases the risk of abuse and more easily rouses desires to use the system beyond the purposes for which it was originally intended. It is therefore necessary to closely scrutinise the Proposals, paying particular attention to the existence of all necessary safeguards.

29 In particular, the Proposals introduce new uses of the data already collected in other systems and changes to the current rights and conditions of access to these data as well as to the architecture of the systems. They imply thus new data processing operations that are not covered by existing legal bases. This has an impact on the fundamental rights to privacy and data protection that needs to be carefully assessed.

3.2 Use of data for new purposes

30 The proposals create a CIR that will contain an individual file for each person recorded in at least one the following systems: EES, VIS, ETIAS, Eurodac and ECRIS-TCN. The individual file will compile data that are recorded in the different systems about this person (except the ones stored in the SIS due to technical reasons). These data will consist of biographical data (names, surnames, place and date of birth, sex, nationalities, travel documents) and biometric data (fingerprints and facial images). For each set of data, the CIR will include a reference to the information systems to which the data belongs to. The shared BMS and the MID will enable the cross-matching of the data stored in the CIR as well as those stored in the SIS.

31 As a preliminary remark, the EDPS would like to stress that the CIR will store data about all third country nationals that have crossed or are considering crossing the EU borders (with a few exceptions), i.e. millions of people. These data include biometric data which are, by nature, very sensitive. Indeed, unlike other personal data, biometric data are neither given by a third party nor chosen by the individual; they are immanent to the body itself and refer uniquely and permanently to a person. Besides, a database is all the more vulnerable, sought-after and subject to multiple uses as it is large, connected to thousands of access points and it stores sensitive data such as biometric data.

32 Due to its scale and the nature of the data stored in a centralised database, the consequences of any data breach affecting the CIR could seriously harm a potentially large number of individuals. If ever it falls into the wrong hands, the CIR could become a dangerous tool against fundamental rights if it is not surrounded by strict and sufficient legal, technical and organizational safeguards. Special vigilance is therefore essential both as regards the purposes of the CIR as well as its conditions and modalities of use.

33 The EDPS recalls that while the systems that will feed the CIR have been built to assist border management and/or law enforcement[22], each of them has been built for a very specific purpose (e.g. EES to identify overstayers, the Eurodac system to determine the Member State responsible for examining an asylum request, etc.).

34 He notes that the Proposals provide for the possibility to use the systems more extensively, i.e. beyond the specific purposes for which they have been established. In particular, the data stored in the different systems will be gathered in order to combat identity fraud but also to facilitate and allow identity checks within Member States' territory.

3.2.1 Combat identity fraud

35 One of the main objectives of the Proposals, according to its impact assessment, is to combat identity fraud. The EDPS recognises that the fight against identity fraud is a legitimate objective of public interest. However, as already stressed above, the solution proposed, i.e. the creation of a database with information about millions of third-country nationals, including their biometric data, appears very intrusive from the point of view of the fundamental rights to privacy and data protection. As reflected in Recital 38, the new data processing operations aiming at correctly identifying the persons constitute an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter. Consequently, they must pass the necessity and proportionality tests (Article 52(1) of the Charter).

36 As recalled in the EDPS' reflection paper, the problems the Proposals aim to address need to be sufficiently and clearly described and accompanied by evidence. The EDPS notes that the impact assessment merely mentions that information provided by the EU systems is not always complete, accurate and reliable. It associates this (without further explanations) to the lack of connections between data in the various systems which, in turn, makes it very difficult to detect multiple identities or to combat identity fraud.[23.] The impact assessment focuses on the likelihood of identity fraud and the difficulties to detect potential fraud but neither explains or estimates the scale of the problem nor provides for cases of identity fraud competent authorities have been confronted with. Without further indications on the existence of identity fraud, it is difficult to ensure that the measure proposed is appropriate and proportionate.

3.2.2 Facilitate the identification of a person during identity checks (Article 20)

37 Article 20 of the Proposals provides that a Member State police authority may query the CIR with the biometric data of a person taken during an identity check solely for the purpose of identifying this person. Such access must be provided by national law. The law shall specify the precise purposes of the identity checks within the framework (as part) of preventing and combating irregular migration and/or contributing to a high level of security. It shall also designate the police authorities competent and lay down the procedures, conditions and criteria of the checks.

38 To justify the need for such use, the impact assessment underlines that, while Member States authorities keep registers of EU nationals and EU residents, they cannot keep complete registers on third country nationals present for a short stay, as those third

country nationals can enter, travel, and exit through different Member States. The CIR could address this gap by allowing access for Member State authorities to the Eurodac system, the VIS, the EES, the ETIAS and the ECRIS-TCN for the purpose of identification of persons in the territory of the EU and enable them to carry out correctly and efficiently their different tasks and obligations.[24]

39 The EDPS would like to stress once more that the identification of a person is not an end in and of itself but needs to serve a specific objective; for instance to check whether the person is wanted by the police or has the right to stay in EU (e.g. is in possession of a valid visa).

40 He notes that under Article 20 the identification of the person must contribute to preventing and combating irregular migration or to contribute to a high level of security within the area of freedom, security and justice including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States. In other words, using the data in the CIR to identify a person would be allowed when it is necessary to combat irregular migration and to contribute to a high level of security.

41 The EDPS stresses that "combating irregular migration and ensuring a high level of security" is a very broad description of (otherwise legitimate) purposes. He notes that Article 20 requires the adoption of a national law that shall further define them. However, he would like to recall that the Court of Justice of the European Union ('CJEU') in its Digital Rights Ireland ruling held that the Directive 2006/24 failed to '*lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offence*s' by simply referring '*in a general manner to serious crime, as defined by each Member State in its national law.'* [25] The Court also considered that the purpose for the access and use of the data was not '*strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto*'[26].

42 **The EDPS considers that the purposes of combating irregular migration and contributing to a high level of security in the context of Article 20 are too broad and do not fulfil the requirements of being '*strictly restricted'* and '*precisely defined*' in the Proposals, as required by the Court. He therefore recommends to further define them in the Proposals**. For instance, "irregular migration" could refer to the conditions of entry and stay as set out in Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council. As regards security, the EDPS recommends to target the criminal offences that could in particular threaten a high level of security; for instance by referring to the crimes listed in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

43 As regards the conditions of access to the data stored in the CIR, the EDPS stresses that in its Digital rights Ireland ruling, the Court also criticized that the '*Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use*' since '*it merely provides that each Member State is to define the procedures to be followed and the*

*conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements***.**'[27]

44 The EDPS notes that Article 20 provides for some conditions and criteria since it limits the access to police authorities and solely for the purpose of identifying a person during an identity check. However he considers that these conditions should be further defined in the Proposals to comply with the requirements of the Court. **The EDPS considers 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) exist and under equivalent conditions. He recommends to make this clear in the Proposals**. Otherwise, the Proposals would clearly seem to establish a presumption that third country nationals constitute by definition a security threat.

45 Furthermore he stresses that an identity check usually consists of a police authority asking individuals, under the legal requirements defined in national law, to proof their identity by any appropriate means such as their identity card or any other valid document.

46 In this context, he notes that Article 20(1) provides that where biometric data of the person cannot be used or the query with that data fails, the query shall be carried out with identity data in combination with the travel document or with the identity data provided by the person. This implies that the identity check would be carried out first on the basis of biometric data and only in case of failure on the basis of other data such as names and travel document. In the view of the EDPS, the consultation of the CIR to identify a person during an identity check should only be carried out on the basis of biometric data as a last resort, i.e.:

- when the person is unable to cooperate (e.g. the person does not understand what she/he is asked to provide for) and does not have document establishing his/her identity or,
- refuses to cooperate or,
- there are justified or well-founded suspicions that documents are false or that the person is not telling the truth about his/her identity.

47 Taking systematically biometric data of a person during an identity check would create the risk of stigmatising certain people (or groups of people) based on their appearance and create unjustified difference of treatment between EU citizens and third country nationals.

48 **Therefore, the EDPS recommends to amend Article 20 to provide that access to the CIR will 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**.

3.2.3 Use of the proposed ECRIS-TCN

49 As a preliminary remark, the EDPS would like to stress that the ECRIS- TCN does not exist yet. The Proposal establishing it[28] is currently being discussed by the EU legislators.

50 The EDPS notes that under Articles 17 and 18 of the Proposal police and judicial cooperation, asylum and migration, the CIR would include the following data stored in the ECRIS-TCN: surname or family name; first name(s) (given name(s)); sex; date of birth; place and country of birth; nationality or nationalities; gender and where applicable previous names, pseudonyms (s) and or alias names(s); facial image; fingerprint data as well as the reference of the number of the fingerprint data of the convicted person including the code of the convicting Member State. As a result, these data could be accessed and used for the purposes of the CIR, namely the facilitation of identity checks and the detection of mulitple identites.

51 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. The argument that the CIR should include data contained in the proposed ECRIS-TCN system as the identities of third-country nationals stored in this system are verified by a judicial authority[29] - and thus are more reliable – does not appear sufficient to pass the necessity and proportionality tests of Article 52(1) of the Charter.

52 Furthermore, the EDPS recalls that the ECRIS-TCN aims at enhancing judicial cooperation in criminal matters by improving the exchange of information on criminal records throughout the EU. Article 22 of the Proposal establishing the ECRIS-TCN[30] specifically provides that the data included in the system shall only be processed for the purpose of the identification of the Member State(s) holding the criminal records information of third country nationals. Using the data stored in the proposed ECRIS-TCN to detect multiple identities and to facilitate identity checks appear to go far beyond the purposes of the ECRIS-TCN as defined in its proposed legal instrument and raises the issue of its compatibility with the purpose limitation principle.

53 **The EDPS therefore recommends to ensure in the Proposals that the data stored in the ECRIS-TCN could only be accessed and used solely for the purposes of the ECRIS-TCN as defined in its founding legal act.**

3.3 Facilitating access to the data for law enforcement purposes (Article 22)

54 The possibility to use the identity data recorded in the EES, the VIS, the ETIAS or the Eurodac system to prevent, detect and investigate terrorist offences or serious criminal offences is not new. This possibility is provided in the (existing or under negotiations) founding instruments of these systems. However, the Proposals introduce significant changes to the conditions of access to these data provided in these instruments.

55 The EDPS has repeatedly stressed his concerns about the general trend observed in the EU in the past years of granting law enforcement authorities access to systems built for other purposes than law enforcement purposes. Should the need for such an access be demonstrated, he has insisted that it should not be granted systematically but only in specific circumstances, on a case by case basis and under strict conditions. These

conditions include that requests for accessing the data are narrowly targeted and based on suspicions on specific persons. [31]

56 Article 22 (1) of the Proposals states that for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, law enforcement authorities and Europol could in a specific case consult the CIR to obtain information on whether data on a specific person is present in the EES, the VIS, the ETIAS or the Eurodac system.

57 The query of the CIR would follow a two-step consultation approach: initially only a reference indicating a system ("hit/no hit) is provided, with full access only granted at a later stage. In case the data contained in the query match with data recorded in at least one of the systems, a hit-flag will appear indicating which system(s) is (are) concerned. (Article 22 (3) first-level query). However, full access to the data would remain subject to the conditions and procedures laid down in the respective legislative instrument governing such access (Article 22 (4), second-level query).

58 The EDPS recognises that a "hit-flag" is limited information. However, contrary to what Recital 33 states, a "hit-flag" consists of information relating to an identified (or identifiable) person and thus constitutes personal data. As already stressed in his reflection paper, the EDPS recalls that the existence (or lack) of a "hit" must always be regarded as personal data, given that even with the absolute minimum of information (e.g. known or unknown in a given system) a "hit" or "no-hit" amounts to information related to a person (e.g. the person is or is not an asylum seeker). As a consequence the processing of such data constitutes an interference with the fundamental rights as protected by Articles 7 and 8 of the Charter and must comply with Article 52(1) of the Charter in terms of necessity and proportionality.

59 Referring to the different access conditions and safeguards governing each system, the explanatory memorandum stresses that some of the current rules could hinder the speed of the legitimate use of the systems by law enforcement authorities. Through the first level query, the Proposals actually would ease the conditions and the modalities of access granted to law enforcement authorities for law enforcement purposes.

60 The EDPS stresses that currently all founding (existing and proposed) instruments of the concerned systems provide for the following cumulative conditions of access:

- access must be necessary for the prevention, detection, or investigation of terrorist offences or other serious criminal offences,
- access must be necessary in a specific case,
- there are reasonable grounds to consider that consultation will substantially contribute to the prevention, detection or investigation of the criminal offences in question.

Besides, the different instruments also require the verification by an independent authority that the above conditions are met prior to the access. In case of the ETIAS, the EES, and the Eurodac system, the law enforcement authorities are also required to first consult other relevant systems (e.g. national databases, Europol data, Prüm, the VIS).

61 The Impact Assessment asserts that this "cascade mechanism" (i.e. obligation of prior verification and prior consultation) creates a considerable amount of administrative

burden and results in delays as well as missed opportunities to uncover necessary information. It mentions that the cascade requires the law enforcement authority to end its query once information is found in one system. However, this does not mean that the next or even a later system in the cascade could not also contain valuable information for law enforcement purposes[32].

62 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, facilitating the access by law enforcement authorities to non-law enforcement systems (even to limited information such as a hit/no hit) is far from insignificant from a fundamental rights perspective. One must bear in mind that those systems have been set up and developed in view of the application of specific policies and not as a law enforcement tool. Routine access would represent a violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of for instance travellers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted for that purpose. Moreover, removing genuine safeguards introduced to preserve fundamental rights mainly in the interest of speeding up a procedure would not be acceptable. If there is a need to improve the procedure, this should not be done at the expense of safeguards.

63 The EDPS notes that it follows from Article 22 of the Proposals that one of the primary conditions to access the systems no longer applies, i.e. the reasonable grounds to consider that consultation will substantially contribute to the prevention, detection or investigation of a terrorist offence or of other serious criminal offences. A reasonable ground could for instance be a fake travel document found on a scene of a crime. He considers that the requirement to have reasonable grounds is a fundamental pre-requisite of any access by law enforcement authorities to non-law enforcement systems. This is indeed an essential safeguard against possible 'fishing expeditions'.

64 Furthermore, the EDPS is not convinced that a prior search in the national databases is such an obstacle. One might reasonably think that law enforcement authorities will first check their own national (criminal) databases to which they have direct access. If the person is undoubtedly identified as an EU citizen, the EDPS doesn't see the need to further check the CIR. The prior search in the national databases should then remain a pre-requisite to access the CIR while it would not automatically prevent subsequent access to the CIR if the other conditions are complied with (i.e., specific case, law enforcement purposes and reasonable grounds).

65 The EDPS also wonders why the consultation of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA ('Prüm Decision')[33] would no longer applies. The EDPS recalls that with the Prüm Decision[34] a specific law enforcement system exists today, which aims at enabling the exchange of police information including fingerprints data to step up cross-border cooperation between the Member States' police and judicial authorities to combat terrorism and cross-border crime. Issues as regards its effectiveness due to (amongst others) the lack of its full implementation or use by the Member States cannot be considered as a valid ground to facilitate access by law enforcement authorities to non-law enforcement systems. In the EDPS 'view, the consultation of other systems under the Prüm Decision should remain a condition of access to the CIR and be carried out at least in parallel to the consultation of the CIR.

66 Consequently, the EDPS considers that access to the CIR to detect whether data on a specific person is present in one of the systems connected to the CIR ("hit/no hit" information) should only be allowed under the following conditions:

- for the purposes of the prevention, detection or investigation of a terrorist offences or another serious criminal offences,
- in a specific case,
- where reasonable grounds exist that the consultation will substantially contribute to the prevention, detection or investigation of the terrorist of other serious criminal offences; in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under the category of third country nationals whose data are stored in the EES, the VIS, the ETIAS and the Eurodac system and,
- a prior search in the national databases has been carried out and a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA has been launched.

67 The EDPS considers that all the above conditions should be mentioned in Article 22 of the Proposals. He notes that Article 22(1) only refers to the conditions of law enforcement purposes and a specific case. **He therefore recommends to add in Article 22(1) 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**. The EDPS further takes note that under Article 22(4), in case of a "hit", full access to the data contained in the system shall remain subject the conditions and procedures laid down in the respective legislative instruments governing such access.

68 Besides, since a "hit" constitutes personal data, the EDPS considers that the compliance with the conditions of access should always be verified, independently of further access to the data stored in the system that triggered the hit. **In other words, the law enforcement authority getting a hit should always refer to the verifying authority that shall check whether the conditions of accessing the CIR were complied with. In case the ex post independent verification determines that the consultation of the CIR was not justified, the authority shall erase all data originating from the CIR. We recommend to amend Article 22 of the Proposals accordingly.**

3.4 Privacy by design and by default

69 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. Nevertheless, the EDPS stresses that the data protection principles should be taken into account during all stages of the implementation of the Proposals.

70 In this regard the EDPS wants to draw attention to the imminent entry into application of the Regulation 2016/679[35] and in particular to the introduction of the concept of data protection by design and by default in its Article 25. The EDPS recalls that this concept will also be introduced in Article 27 of the new Regulation (EC) 45/2001[36].

71 This concept requires that eu-LISA and the Member States should implement appropriate technical and organisational measures in order to effectively ensure compliance with the data protection principles and to integrate the necessary safeguards to meet the requirements of the GDPR and in particular to protect the rights of data subjects. Moreover, eu-LISA and the Member States should ensure that by default only those personal data are processed, which are necessary for each specific purpose of the processing.

72 The EDPS recommends to include in the Proposals a reference to the obligation for eu-LISA and the Member States to follow the principles of data protection by design and by default.

4. Specific recommendations

4.1 Reference to applicable data protection legislation

73 As a preliminary remark, the EDPS observes that some Articles of the Proposals refer to certain provisions of the applicable data protection legislation (i.e. the Regulation 2016/679, the Directive 2016/680 and the Regulation 45/2001), e.g. Articles 46 and 47 of the Proposals. The EDPS understands that these provisions aims at further specifying the relevant articles of the aforementioned legal acts. However to make it clear that these references are without prejudice to the application of other relevant provisions of these legal acts, **the EDPS recommends to provide for a provision in the Proposals on the applicability of Regulation 2016/679, Directive 2016/680 and Regulation 45/2001.**

4.2 User profiles for ESP

74 The EDPS welcomes the fact that the Proposals provide a central management on the creation of user profiles with allocation of the legal access rights. However, he stresses that **these profiles should be regularly reviewed and if necessary updated. The EDPS recommends to add this obligation in the text of the Proposals**.

75 In Article 7(4) of the Proposals it is defined which EU bodies can access the ESP. **The EDPS recommends to add after EU bodies the text "as referred to in paragraph 1**".

76 In Article 8(1) of the Proposals it is defined that every category of user profile shall be linked with three elements: the fields of data that can be queried, the systems that can be consulted and the data that can be provided in each reply. The EDPS is of the opinion that the purpose of the query is equally important which is, however, not included in the Article. Therefore, **the EDPS recommends to add in Article 8 of the Proposals also a reference to the purpose of the query**.

4.3 The shared BMS - Categories of data

77 The EDPS understands that in accordance with recital 17 of the Proposals the purpose of the shared BMS is to regroup and store all biometric templates in one single location to facilitate cross-system comparisons using biometric data in order to detect multiple identities, in particular via the CIR. In this context, Article 13 of the Proposals lists all relevant biometric data that should be stored in the shared BMS.

78 As regards the VIS, Article 13(1)(b) of the Proposals determines that the shared BMS should retain only the biometric template from the fingerprints of the VIS applicants. However, Article 18(1)(b) of the Proposal "Border on Border and Visa provides that also the photograph of the VIS applicant should be stored. The EDPS understands that the photograph of the VIS applicant is a relevant biometric data in terms of Article 13, which would add significant improvement to the detection of multiple identities. Therefore, **the EDPS wonders why the photograph of the VIS applicant is not included in Article 13(1)(b) of the Proposals**.

79 With regard to the SIS, Article 13(1)(c) of the Proposals refers to Article 20(2)(w) and (x) of the Proposal for Regulation on SIS II in the field of law enforcement. However, the definition of dactylographic data in the SIS Proposal also encompasses palm prints. The EDPS recommends to clarify in the Proposals that the reference to dactylographic data in the SIS should only include fingerprints and not palm prints. Furthermore, he observes that in the context of the SIS Proposal of a Regulation in the field of law enforcement, Article 13(1)(d) of the Proposals refers to Article 20(3)(w) and (x) Proposal for Regulation on SIS II in the field of law enforcement. The EDPS points out that Article 20(3)(x) of the Proposal of a Regulation in the field of law enforcement explicitly refers to DNA data. **Therefore, the EDPS recommends to change Article 13(1) (c) and 13(1)(d) of the Proposals to ensure that neither the DNA data nor the palm prints will be stored in the shared BMS.**

80 **With regard to Article 16(1)(d) of the Proposals the EDPS recommends to provide a definition on the length of the query, since the term is not self-explanatory**.

4.4 The CIR - Duplication of records

81 In the explanatory memorandum it is stressed that one of the Proposals aims is to provide simplicity and reduction of duplication.[37] The EDPS expects that the CIR will therefore support a single entry of data concerning an individual when identical personal data are recorded or corrected in the different systems. However, this is not clear when Article 17 and Article 18 of the Proposals are read together.

82 While Article 17 of the Proposals stipulates that an individual file is created in the CIR for each person that is recorded in any of the systems, Article 18 of the Proposals only provides a list with the relevant data that should be stored in the CIR. This means that when an individual has several identical records in one of the underlying systems, the CIR will also retrieve these identical data. Moreover, Article 23(2) of the Proposals states that an individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the underlying information systems.

83 Therefore, **the EDPS is concerned that the Proposals do not sufficiently prevent the possibility of duplication of personal data. He therefore recommends to be more specific in the relevant Articles and make the necessary changes**.

4.5 Data retention period in the CIR and MID

84 Article 23(2) and Article 35 of the Proposals define the retention period of the data stored in the CIR and MID, respectively. An individual file shall be deleted from the CIR only when the corresponding data are deleted from all information systems. The identity confirmation files and its data with the links will be stored in the MID as long as the linked data is stored in two or more information systems.

85 However, the Proposals do not specify the method of deletion of data after their expiration. There is a risk that when information is entered in a system for a specific period - unless the retention period and automatic deletion is technically enforced by the system - personal data may be retained in the system beyond the date by which the data should have been deleted. **Therefore, the EDPS recommends to specify in the relevant Articles that automatic deletion of data will apply**.

4.6 Manual verification of links

4.6.1. Automated decision-making

86 The EDPS wants to draw the attention that the automated process of creating links for the purpose of multiple-identity detection would constitute automated decision-making within the meaning of data protection law. Data protection rules traditionally grants individuals a high level of protection in such circumstances, given the lack of human intervention and potential intrusiveness into the private sphere. For example, Article 22 of the Regulation 2016/679 and Article 19 of Regulation (EC) No 45/2001 provide in this respect, that a data subject has the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her without any human intervention.

87 Although Article 22(2) of the Regulation 2016/679 and Article 19 of Regulation (EC) No 45/2001 provides that this right can be limited by law, the EDPS wants to recall that such law must at the same time "lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". In order to ensure fair and transparent processing in respect of the data subject under such circumstances, the logic of the decision-making and any consequences must be clearly explained to the individuals concerned (see Articles 13(2)(f) and 14(2)(g) Regulation 2016/679). The controller should also use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect[38].

88 Therefore, **the EDPS considers that the process of creating links for the purpose of multiple-identity detection would constitute automated decision-making. Consequently, transparency towards the individuals affected and the necessary safeguards for such processing, should be provided for in the Proposals.**

4.6.2. Manual verification

89 The Proposals introduce a multiple identity detector ("MID") that will be able to indicate whether a person is known under different identities in the different information systems (i.e. the SIS, VIS, ETIAS, ECRIS, EES or Eurodac). The MID will store links between the individuals present in more than one system as well as the reference to the system to which the data belong to. These links will be labelled in four categories: white, yellow, green and red:

- a white link means that the different biographical identities belong to the same person.
- a yellow link means that there are potential differing biographical identities on the same person.
- a green link confirms that different persons happen to share the same biographical identity or,
- a red link means that there are suspicions that different biographical identities are unlawfully used by the same person.

90 Article 28(4) of the Proposals provides that a yellow link is created when a query of biometric data or identity data leads to one or several hits and the identity data of the linked files cannot be considered as similar. However, Article 30(1)(b) of the Proposals state that a yellow link is created when the linked data has different identity data and no manual verification has taken place. This definition is rather confusing, since it implies that between all different data of two or more information systems a yellow link would be created. This would also mean that no green link could be created by the authority responsible, since no yellow link would have been created beforehand. **The EDPS assumes that instead of "different data" it is meant "similar data" and recommend to change Article 30 accordingly. For the sake of clarity, he moreover recommends, to provide in Article 28(4) and Article 30 of the Proposals a uniform definition of a "yellow link".**

91 The creation of a yellow link triggers the manual verification procedure as laid down in Article 29 of the Proposals. Article 29(1) of the Proposals provides that the manual verification should be carried out by the authority which created or updated the relevant file. In contrast, Article 29(2) of the Proposals foresees an exclusive responsibility by the Sirene Bureaux when a yellow link refers to a SIS-alert. Since the Sirene Bureau is not necessarily involved in the creation or update of a file in the sense of Article 29(1) of the Proposals, it is not clear whether and how the Sirene Bureau could be informed of its responsibility to verify the different identities. **The EDPS recommends to add in Article 29 of the Proposals that the responsible Sirene Bureau is immediately informed when a yellow link has to be manually verified by it.**

92 In this respect, the EDPS observes that Article 29 of the Proposals provides that the authorities responsible should update the relevant links without delay, however, there are no provisions dealing with the case where an authority responsible does not comply with its responsibilities. **The EDPS therefore recommends to introduce a fixed timeframe with specific deadlines and establish a clear procedure to guarantee a timely verification, since such links could potentially have adverse consequences for the person(s) concerned.**

93 In accordance with Article 29(3) of the Proposals, the authority responsible should access the relevant identity confirmation file in the MID and in accordance with Article 21 of the Proposals the identity data linked in the CIR in order to verify the identity of a person. In regard to the CIR, Article 21 of the Proposals clarifies that access should only be granted to the identity data connected to a yellow link. The authority responsible will then have to assess the different identities and decide whether the link can be regarded as a green, a red or a white link. When the decision of the authority responsible leads to a white or red link, the new data is in accordance with Article 19(2) of the Proposals added to the individual file in the CIR.

94 Under Article 27(1)(e) of the Proposals the MID is launched when an alert on a person is created or updated in the SIS. However, Article 26(1)(e) and Article 29(1)(e) of the Proposals provide that the Sirene Bureau would only get access to the MID when it updates an alert but not when it creates an alert. **The EDPS sees this as an editorial error and recommends to change Article 26 and 29 of the Proposals accordingly.**

95 Furthermore, the EDPS observes that the Proposals often speak about different identities that refer lawfully or unlawfully to a person (Article 32(1)(a) (b)). **Since the Proposals do not elaborate when an identity refers lawfully or unlawfully to a person, the EDPS recommends to further clarify the meaning of these terms in the relevant provisions or at least in a recital**.

96 Finally, the EDPS observes that the Proposals foresee the possibility for a data subject to correct a factually incorrect link, but there is no possibility for the Member States themselves to rectify such links[39]. The EDPS is of the opinion that such a mechanism would further improve the data quality within the relevant systems and thus serve the envisaged objective of interoperability. Therefore, **he recommends to adopt in the Proposals a relevant mechanism under which the Member States themselves can rectify an incorrectly set link**.

4.7 Central repository for reporting and statistics - CRRS

97 Pursuant to Article 39 of the Proposals, eu-LISA should establish, implement and host a central repository for reporting and statistics. The EDPS recalls in this context his previous Opinions on the EES[40], ETIAS[41], the SIS[42] and eu-LISA[43]. In these Opinions, the EDPS strongly cautioned that the proposed solution for providing statistics would impose a heavy responsibility on eu-LISA and on the EDPS, since eu-LISA would have to maintain and secure a second repository, while the EDPS would have to supervise this second repository.

98 Therefore, the EDPS would favour a solution that does not require an additional central repository but rather requires eu-LISA to develop functionalities that would allow the Member States, the Commission, eu-LISA, as well as the authorised authorities to automatically extract the required statistics directly from the system.

99 In this respect the EDPS stresses that eu-LISA should also perform a thorough information security risk assessment before the implementation of the CRRS and also address the issue of secure access points. It is important, that adequate security measures shall be in place prior to the establishment of the CRRS.

100 The EDPS understands the need for the duly authorised staff of the competent authorities of the Member States, the Commission and eu-LISA to have access to data contained in the CIR and the MID for the purpose of reporting and statistics and for the European Border and Coast Guard Agency for the purpose of risk analysis and vulnerability assessments. However, it should be noted that contrary to the wording in Article 56(2) and (3) of the Proposals the combination of nationality, gender and date of a person could lead to individual identification.

101 **The EDPS therefore recommends to redraft Article 56(2) and (3) of the Proposals and to recognise that the data listed under Article 56(2)(a) to (d) and (3)(a) to (c) may lead to identification of individuals and therefore must be protected. This includes once again, performing a thorough information security risk assessment, and implementing adequate security measures, prior to providing this additional central repository. The EDPS also recommends that privacy by design should also be applied when designing the CRRS**.

4.8 Qualification of eu-LISA as processor

102 The EDPS has pointed out in several occasions the implications of the distribution of roles amongst several actors in EU large-scale databases and recommended that where an actor independently defines purposes or means of the data processing it should be considered controller rather than processor[44]. In the same vein, where multiple entities contribute to the purposes and/or means of processing, as it is the case in this Proposal for a Regulation, they should be considered as joint controllers.

103 Article 4(7) of Regulation 2016/679 defines controller as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Article 26 of Regulation 2016/679 elaborates the notion of joint controllership and states that where two or more entities jointly determine the purposes and means of processing these are considered to be joint controllers. These joint controllers should clearly define who is responsible for what between them where this is not already defined by law.

104 The Article 29 Working Party issued in 2010 an opinion on the concept of controller, processor, as well as, joint controllership.[45] In its opinion, the Article 29 Working Party concluded that the concept of controller is autonomous, in the sense that it should be interpreted mainly according to Union data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis.

105 Article 40 of the Proposals states that the Member States authorities that are the controllers of the relevant source systems remain controller of the shared BMS and the CIR. For the processing of data in the MID the European Border and Coast Guard Agency and the Member State authorities adding or modifying the data in the identity confirmation file are considered to be controllers in accordance with Regulation (EU) 2016/679. Article 41 of the Proposal for a Regulation states that eu-LISA is to be considered the data processor in accordance with Regulation (EC) No 45/2001 for the processing of personal data in in the CIR.

106 According to Article 52 of the Proposals, eu-LISA will be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems and the European search portal, the shared BMS, the CIR and the MID. Moreover, eu-LISA shall define the physical architecture, including its technical specifications, whereby representatives of Member States assembled in a Programme Management Board shall ensure the adequate management of the design and development phase (Article 52(4)). The technical management of the central infrastructure lies with eu-LISA, which is also responsible to ensure the security of the interoperability components and their related communication infrastructure (Article 53(1) and Article 42(2)). Eu-LISA in cooperation with the Member States shall ensure the best available technology (Article 53(1), whereas eu-LISA shall also develop and maintain a mechanism for data quality checks (Article 53(3)). This shows that eu-LISA will have an important role in determining the means of the processing, both during initial development and during operations.

107 As explained above, the concept of controllership is based on a factual analysis. The assignment of roles in the Proposal for a Regulation leads to a situation where Member States are responsible for matters their control (e.g. how eu-LISA manages information security and secure transmission of the data to and from the databases). Additionally, eu-LISA receives tasks (developing the system, ensuring its security during operations etc.) that according to the proposals, it is meant to fulfil with greater autonomy than that of a processor. Therefore, **we recommend designating eu-LISA and the competent authorities of the Member States as joint controllers, each with their clearly defined tasks and responsibilities.**

4.9 Security

108 The EDPS notes that the Proposals would bring together large-scale EU databases with sensitive data. Therefore, it is utterly important that these data are protected against any possible attackers and security incidents. The EDPS strongly recommends that eu-LISA and the Member States should take into account the principle of data protection by design and by default during the development and implementation phase of every new system and interoperability component and moreover, implement a comprehensive Information Security Risk Management Process (ISRM).

109 The EDPS stresses the importance of performing a comprehensive information security risk management following Article 22 of Regulation (EC) No 45/2001 and the EDPS's guidance. The EDPS recommends that every reference to information security or security plans in the Proposal should be replaced by, 'the implementation of a comprehensive Information Security Risk Management Process (ISRM)'.

110 Pursuant to Article 37 of the Proposals, automated data quality checks shall ensure a minimum level of data quality for all the data stored in the systems. The EDPS welcomes the establishment of such automated data quality checks. However, when paragraph (1) and (3) of Article 53 of the Proposals are read in conjunction, it follows that eu-LISA will develop a mechanism to carry out such quality checks only after the new systems are operational.

111 **The EDPS strongly recommends that automated data quality checks are established as soon as possible and preferably already tested before the entry into operations.**

112 The EDPS is of the opinion that eu-LISA should address also the issue of security governance during the development phase of the interoperability components, since this will ensure the application of state of the art security measures.

113 Article 42 of the Proposals defines the security of processing for both eu-LISA and the Member States. The EDPS is of the opinion, that the technical responsibilities for the security of the interoperability components should be shared between eu-LISA and Member States taking into account the specific architectural design of the system. **While the Member States' authorities cannot be responsible for the central system, they can be responsible for the security at the end-points in regard to the access to the systems (security of their national communication lines, access controls, authorizations, data processing, etc.). The EDPS recommends to amend Article 42(1) of the Proposals to reflect this distinction.**

114 The EDPS recalls that an adequate security plan as defined in Article 42(3) of the Proposals should be the result of a thorough information security risk assessment, which is why a relevant reference should be made in Article 42(3) of the Proposals. The security plan should also define exactly the responsibilities and requirements of security for each stakeholder. In general, it is important to remember that effective information security can only be achieved through a thorough analysis of the information security risks an information system is subject to.

115 As reflected in Article 42(3)(i) of the Proposals, the security measures have to be monitored by eu-LISA which also has to take the necessary organisational measures. **The EDPS suggests to enhance this provision in order to allow the establishment of a security governance system that will assess the applied security measures taking into account also new technological developments.**

4.10 Data subject rights

116 The EDPS takes note that the Proposals refer in terms of data subjects' rights to the relevant provisions in the Regulation (EC) 45/2001 and the Regulation (EU) 2016/679. Nevertheless, the primary objective of the ECRIS and partly the SIS is law enforcement and judicial cooperation, where Directive 2016/680 applies. In this respect, the EDPS recommends to include in Article 46 of the Proposals a reference to Article 13 of Directive 2016/680 and in Article 47 of the Proposals a reference to Article 14 and 16 of the Directive 2016/680.

117 Article 46 of the Proposals provides that the competent authorities should inform the data subjects about the processing of their personal data in the shared BMS, the CIR and the MID, their purpose, the identity and contact details of the controller, the procedures for exercising their data protection rights and the contact details of the EDPS and the national supervisory authorities. The EDPS welcomes the fact that data subjects are informed of the presence of multiple unlawful identities (cf. Article 32(4) of the Proposals). However, he takes note that the proposed limitations of the data subjects' right to information are not in line with Article 13(3) of Directive (EU) 680/2016. **Therefore, he recommends to align Article 32(4) of the Proposals with Article 13(3) of Directive (EU) 680/2016.**

118 The EDPS is of the opinion that it is imperative that data subjects should also be informed about the retention period of their data, i.e. that the retention period is subject to the relevant Regulations, as laid down in Article 13(2)(a) of Regulation 2016/679 and Article 13(2)(b) of the Directive 680/2016. Since the automated process of creating links for the purpose of multiple-identity detection constitutes automated decision-making, the data subjects should also be informed thereof (cf. Article 13(2)(f) of Regulation 2016/679). Moreover, the EDPS is of the opinion that data subjects should also be informed about the recipients of their data and in accordance with Article 48 of the Proposals that their data stored in or accessed by the interoperability components are not transferred or made available to third countries, international organisations or private parties with the exception of transfers to Interpol, as laid down in Article 13(1)(f) of the GDPR and Article 13(2)(c) of Directive 680/2016.

119 **The EDPS therefore recommends to add in Article 46 of the Proposals that the data subjects should also be informed about the relevant retention periods, the automated decision-making and the fact that personal data is not transferred or made available to third countries, international organisations or private parties with the exception of transfers to Interpol.**

120 The EDPS observes that Article 47(1) of the Proposals provides with regard to the data subjects' right of access, the rights to rectification, erasure and restriction that the data subject can send his or her request to any Member State, which shall examine and then reply to the relevant request.

121 In this respect, the EDPS observes that when an individual would submit a request to any Member State as it is laid down in Article 47(1) of the Proposals, this Member State would have to assess who is the responsible Member State for the manual verification. However, since Article 13(2) and Article 18(2) of the Proposals merely refer to the relevant system but not the Member State responsible, Article 26(2) limits the access of the Member State to Identification confirmation file in this respect. Therefore, **the EDPS recommends to add in Article 13(2) and Article 18(2) of the Proposals a reference to the Member State responsible and with regard to Article 26(2) of the Proposals a reference to Article 34(d).This way, it would be ensured that the data subject can effectively exercise his or her rights**.

122 With regard to Article 47(3) of the Proposals, the EDPS observes that this paragraph only refers to the right to correction and erasure, but not to the right to restriction. **The EDPS recommends to add the right to restriction in Article 47(3) of the Proposals.**

123 While Article 47(3) of the Proposals foresees that a request for correction and erasure should be forwarded by a Member State to the Member State responsible, there is however no such provision for the right of access. **The EDPS recommends to add in Article 47 of the Proposals a relevant paragraph which should entail an obligation for the Member State to forward the access request to the Member State responsible**.

124 Moreover, **the EDPS recommends to add in Article 47 of the Proposals an obligation for the Member States to inform the data subject that his or her request was forwarded, while indicating the contact details of the competent authority in the relevant Member State**. This would allow the data subject to identify the competent

authority more easily and would enable the data subject to address further requests directly to the responsible authority.

125 **With regard to Article 47(4) of the Proposals the EDPS recommends to include an obligation for the Member State to immediately inform the data subject after his or her data were corrected or deleted**.

126 Finally, the EDPS wants to point out that the interoperability components will in their inception phase process mainly data that are already stored in the relevant systems at that moment. Hence, the questions arises how the controllers can provide the data subjects with relevant information prior to the processing. **The EDPS recommends that an adequate awareness rising campaign should be launched by the Member States and at EU level before the interoperability components are implemented and they become fully operational**.

4.11 Access by eu-LISA staff

127 Article 68(3) of the Proposals provides that eu-LISA could have access to all necessary data for the purpose of technical maintenance. Since eu-LISA is the system provider and administrator of all the systems and the interoperability components, the EDPS understands that eu-LISA must have access to personal data stored in the systems.

128 However, **the EDPS recommends to emphasize in Article 68(3) of the Proposals that eu-LISA should only have access to personal data under strict safeguards and for legitimate and specific purposes. In this respect, the Proposals should clearly define relevant situations when the eu-LISA may legally access personal data, as for example when a Member State asks eu-LISA to intervene for deconfliction of data (especially with biometrics) or for support etc. The EDPS therefore asks to explore these circumstances and - if required - amend the Proposals accordingly**.

129 **The EDPS furthermore stresses that any access by eu-LISA should be logged and strongly recommends to insert in the Proposals a relevant provision**.

4.12 Transitional period

130 The EDPS understands that in accordance with recitals 21, 22 and Article 17(2) of the Proposals, the CIR would store the personal data (biographic and biometric data) of third country nationals from the EES, VIS, Eurodac, ETIAS and ECRIS-TCN. It is also clear that these data would not remain in the aforementioned systems, as CIR will be "*a central architecture that shall replace the central systems"*.

131 However, following the Commission's plan and the feasibility study concerning the CIR, a hybrid solution would apply for a certain period of time. Hence, the data that are stored in the CIR would remain in the underlying systems to ensure the proper functioning of the new system. This means that for an undefined period of time there would be a duplication of data.

132 **The EDPS acknowledges the necessity of such a period, however, this hybrid solution should be reflected in the transitional Article of the Proposals and it should be stressed that this hybrid solution should only be in place for a limited time period**.

4.13 Logs

133 The EDPS welcomes that the interoperability components will store logs for the purposes of data protection and monitoring. However, **he recommends that the Proposals should also include provisions that will clarify who shall have access to the logs, and how this access is granted**, since the relevant Article 42 of the Proposals does not provide any additional information concerning the management and access to these logs.

134 The EDPS takes note that according to Article 10(1) and 16(1) of the Proposals, logs of all data processing operations within the ESP and the shared BMS are kept centrally by eu-LISA. Nevertheless, Article 45 of the Proposals obliges the data controllers to take the necessary measures to monitor the compliance of the data processing, including frequent verification of logs, and cooperate, where necessary, with the supervisory authorities as referred to in Articles 49 and 50 of the Proposals.

135 Since neither the Member States as data controllers (cf. Article 40), nor the national supervisory authorities have access to the logs of the ESP and the shared BMS, the EDPS concludes that an adequate verification or supervision of the ESP and the shared BMS is not possible.

136 **The EDPS therefore recommends to store the logs of the ESP and the shared BMS also at national level, as are the logs of the CIR (Article 24(5)) and the MID (Article 36(2)).**

4.14 National supervisory authorities

137 According to Article 49 of the Proposals, the national supervisory authorities should ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every four years. However, the Proposals do not foresee the monitoring of the lawfulness of the processing of personal data under these proposals by the national supervisory authority but rather speaks in Article 45 of a self-monitoring carried out by the data controllers themselves.

138 **The EDPS strongly advises to introduce a provision which states, that each Member State shall ensure that the supervisory authority or authorities designated pursuant to Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680 shall monitor the lawfulness of the processing of personal data under the Proposed Regulations**.

139 **The EDPS recommends to add in Article 44 (3) of the Proposals the national supervisory authority.**

4.15 Role of the EDPS

140 The EDPS is the competent data protection authority to supervise eu-LISA. In order to enable the EDPS to effectively supervise eu-LISA as part of his competencies, he

considers that he should be put in the list of recipients of the reports that eu-LISA has to publish in accordance with Article 68(2) and (4) of the Proposals.

141 Furthermore, the EDPS recalls that supervision can only be effective when he is provided with adequate resources. While Article 49 (2) of the Proposals foresees that the national supervisory authorities should have sufficient resources to fulfil their tasks entrusted to them under this Regulation, **the EDPS recommends to include a similar provision in Article 50 in order to ensure adequate resources for him**.

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,

Giovanni BUTTARELLI

Notes

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 8, 12.1.2001, p. 1.
[4] OJ L 350, 30.12.2008, p. 60.
[5] OJ L 119, 4.5.2016, p. 89.
[6] 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.
[7] Idem, p. 15.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12]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.
[13] https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.
[14] 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, J.O.C.E. L 327/20, 9.12.2017.
[15] 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.
[16] 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.
[17] 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, J.O.C.E., L 135/53.
[18] European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security, annexed to the 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.
[19] See for instance 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 180/1, 29.06.2013.
[20] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017establishing 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 and Eurodac; 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.

[21]Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.

[22] Except the ECRIS- TCN which has been built for purposes of judicial cooperation.

[23] Impact assessment p. 9-10.

[24] Impact assessment p. 39.

[25] CJEU, Digital Rights Ireland Ltd, C-293/12, 8 April 2014, para 60.

[26] CJEU, Digital Rights Ireland Ltd, C-293/12, 8 April 2014, para 61.

[27] CJEU, Digital Rights Ireland Ltd, C-293/12, 8 April 2014, para 6.

[28] Proposal for a Regulation establishing a centralised 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/2017/0344 final.

[29] See impact assessment p. 39.

[30] Proposal for a Regulation establishing a centralised 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/2017/0344 final.

[31] Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final), available at https://edps.europa.eu/sites/edp/files/publication/06-01-20_access_vis_en.pdf, Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (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 the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, available at https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_en.pdf; Opinion 06/2016 on the Second EU smart borders package, recommendations on the revised proposals to establish an Entry-Exit system, p. 19-20, available at https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf , Opinion 3/2017 on the Proposal for a European Travel Authorisation and Information System, p.13 available at: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf .

[32] Impact assessment, p. 25 and 43.

[33] 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.

[34] 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.

[35] 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, O.J.L. 119, 4.5.2016, p. 1.

[36] Proposal for a Regulation of the European Parliament and of the Council 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/E, COM(2017) 8 final.

[37] See Page 12 of the Explanatory Memorandum, COM (2016) 793 final.

[38] Cf. Recital 71 of the GDPR.

[39] See for instance Article 34 (3) SIS II Regulation.

[40] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf.

[41] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf.

[42] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf.

[43] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf.
[44] EDPS Opinion 6/2016 on the Second EU Smart Border Package, para. 70 or the EDPS Opinion 11/2017 on the proposal for a Regulation on ECRIS-TCN, para 42.
[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.