



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 9/2018

on the Proposal for a new Regulation on the Visa Information System



12 December 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 provides for recommendations on how to better safeguard the right to privacy and the protection of personal data in the proposed Regulation..

Executive Summary

In order to enhance security and improve the EU external borders management, the Commission adopted a Proposal which would upgrade the Visa Information System ('VIS'), the EU centralised database that contains information about persons applying for a Schengen visa.

In particular, the Proposal provides for (a) the lowering of the fingerprint age for child applicants for a short stay visa from 12 years to 6 years, (b) the centralisation at EU level of data related to all holders of long stay visas and residence permits and (c) the cross-check of visa applications against other EU information systems in the area of freedom, security and justice.

The EDPS stresses that biometric data such as fingerprints are highly sensitive. Their collection and use should be subject to a strict necessity analysis before deciding to store them in a database where a large number of persons will have their personal data processed. This is even more critical when it concerns fingerprints of children who are particularly vulnerable members of our society and therefore deserve special protection.

The EDPS recognises that strengthening the prevention and fight against children right's abuses such as trafficking is of utmost importance. Nevertheless, he notes that it remains unclear whether or to what extent the child trafficking is rooted in or amplified by the mis- or non-identification of children entering the EU territory on the basis of a visa. Should further elements be provided in support of this claim, the EDPS stresses the importance of ensuring that fingerprints of children would only be used when it is in the best interest of the child. Additionally, appropriate safeguards should be included in the Proposal

Furthermore, the EDPS notes that by including data on all holders of long stay visas and residence permits in the VIS, the Proposal would include the only category of third country nationals that are not currently covered by any of the EU large-scale systems in the area of freedom, security and justice. In the context of the proposed interoperability of EU large-scale systems, the Proposal would contribute to the establishment of an EU centralised network giving access to a considerable amount of information about all third-country nationals that have crossed or are considering crossing the EU borders (i.e. millions of people). He notes that there are two objectives of centralising data related to long stay visas and residence permits: (a) to ascertain the authenticity of a document and the legitimate relation with its holder and (b) to facilitate exchange of information on individuals whose visa request has been refused for security grounds. In this context, he considers that harmonising secure documents should be further investigated and that data stored in the VIS should be limited to individuals whose long stay visa or residence permit has been refused on security grounds.

Finally, the Proposal provides for the comparison of data stored in the VIS with data stored in other systems built and used so far for purposes other than migration. In particular, the data of visa applicants would be compared with data collected and stored for police and judicial cooperation purposes. In line with his concerns about the increasing trend to blur the boundaries between migration management and fight against crime and terrorism, the EDPS notes that the Proposal does not determine clearly how and to which extent police and judicial information has to be taken into consideration in the visa issuance decision making process. He recommends to clarify in the Proposal the purpose of the comparison of the VIS data with police and judicial information as well as the procedure and conditions applicable as regards the outcome of such comparison. He also recommends to ensure in the Proposal that only police and judicial information that are legally part of the visa issuance decision-making process would be accessible to visa authorities.

TABLE OF CONTENTS

1	INTRODUCTION.....	5
1.1	BACKGROUND.....	5
1.2	OBJECTIVES OF THE PROPOSALS.....	6
2	MAIN RECOMMENDATIONS.....	7
2.1	LOWERING THE MINIMUM AGE TO TAKE FINGERPRINTS.....	7
2.2	CENTRALISATION OF DATA RELATED TO LONG STAY VISAS AND RESIDENCE PERMITS.....	9
2.3	CROSS CHECKING WITH DATA STORED IN OTHER SYSTEMS.....	11
2.3.1	<i>ECRIS-TCN</i>	12
2.3.2	<i>Europol data</i>	12
2.3.3	<i>SIS alerts</i>	13
3	SPECIFIC RECOMMENDATIONS.....	14
3.1	CATEGORIES OF VIS DATA COMPARED WITH DATA RECORDED IN OTHER SYSTEMS (NEW ARTICLE 9A(3) OF REGULATION 767/2008).....	14
3.2	SPECIFIC CATEGORIES OF VISA APPLICANTS (NEW ARTICLE 9B OF REGULATION 767/2008).....	15
3.3	DEFINITION OF CENTRAL AUTHORITIES (NEW ARTICLE 9C OF REGULATION 767/2008)....	15
3.4	USE OF VIS DATA TO ENTER A SIS ALERT ON MISSING PERSONS (NEW ARTICLE 20A OF REGULATION 767/2008).....	15
3.5	VERIFICATIONS IN CASE OF A HIT (NEW ARTICLE 22B (6) AND (7) OF REGULATION 767/2008).....	16
3.6	ACCESS FOR LAW ENFORCEMENT PURPOSES (NEW CHAPTER III B OF REGULATION 767/2008).....	17
3.7	STATISTICS.....	18
3.8	USE OF ANONYMISED DATA FOR TESTING PURPOSES.....	19
3.9	DATA QUALITY MONITORING.....	21
3.10	SUPERVISION OF THE VIS.....	21
4	CONCLUSIONS.....	22
	NOTES.....	25

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 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)¹,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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/EC², and in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard 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/JHA³.

HAS ADOPTED THE FOLLOWING OPINION:

1 Introduction

1.1 Background

- 1 On 6 April 2016, the Commission adopted a Communication *Stronger and Smarter Information Systems for Borders and Security*⁴ to launch a discussion on the shortcomings in the functionalities of existing systems for border management and internal security in the European Union in order to optimise their performance.
- 2 On 17 June 2016, the Commission set up a high-level expert group on information systems and interoperability (“HLEG”), which comprised experts in the field of information systems and interoperability, nominated by Member States, Schengen associated countries, and EU agencies and bodies. The objective of the expert group was to contribute to an overall strategic vision on how to make the management and use of data for both border management and security more effective and efficient, in full compliance with fundamental rights, and to identify solutions to implement improvements.⁵
- 3 The HLEG presented its recommendations in its final report in May 2017⁶. With regard to the VIS, the HLEG made several recommendations, inter alia:
 - to extend the scope of the VIS to store long-stay visas and residence documents,
 - to improve access for law enforcement authorities while respecting the highest data protection standards,
 - to improve the data quality in the system, in particular the quality of facial images to allow multimodal searches using biometrics,

- to lower the fingerprinting age for children, to respond to concerns of human trafficking involving children and child abductions, and irregular migration involving minors,
 - to improve VIS capacity in terms of producing statistics and reports relevant for migratory trends and phenomena.⁷
- 4 On 17 August 2017, the Commission launched a public consultation on lowering the fingerprinting age for children in the visa procedure from twelve years to six years.⁸ On 17 November 2017, the Commission launched another public consultation on extending the scope of the Visa Information System (“VIS”) to include data on long stay visas and residence documents.⁹ The EDPS participated in both public consultations and issued two statements.¹⁰
- 5 On 15 May 2018, the Commission published a proposal (hereinafter “the Proposal”) for a Regulation of the European Parliament and of the Council amending:
- Regulation (EC) No 767/2008 (“*VIS Regulation*”),
 - Regulation (EC) No 810/2009 (“*Visa Code*”),
 - Regulation (EU) 2017/2226 (“*EES Regulation*”),
 - Regulation (EU) 2016/399 (“*Schengen Border Code*”),
 - Regulation XX/2018 (Interoperability Regulation),
 - and Decision 2004/512/EC (“*VIS Decision*”),
 - and repealing Council Decision 2008/633/JHA (“*Law enforcement access Decision*”).
- 6 The EDPS has been invited to contribute to the two public consultations launched by the Commission (see supra point 4). Since the Proposal relies to a major extent on the processing of personal data, he wonders why he hasn’t been consulted on it by the Commission, either informally or formally.

1.2 Objectives of the Proposals

- 7 The Proposal aims at improving security within the Union and its borders and at facilitating the management of the Schengen external borders. In particular, the Proposal aims to improve the visa processing, expand the use of the VIS for new categories of data, make full use of the interoperability instruments, improve the data quality and enhance the VIS system.
- 8 To this end, the Proposal introduces the possibilities to:
- Include long stay visas and residence permits in the VIS, in order to:
 - o ascertain the authenticity and the validity of the document and the legitimate relation with the holder,
 - o facilitate the exchange of information between Members States enabling them to check whether the person is not a threat to the security of the Member States before or when the person reaches the external border.
 - Lower the fingerprint age for child applicants for a short stay visa from 12 years to 6 years in order to verify the identity of a child holding a visa at the border and to contribute to the fight against human trafficking.
 - Check all visa applications recorded in the VIS against all other EU information systems in the area of freedom, security and justice using interoperability to increase security checks.

- Store a copy of the bio-page of the applicants travel document in the VIS as evidence to support procedure to return irregular migrants to their countries of origin in case travel documents are missing.
 - Use fingerprints stored in the VIS for entering alerts on missing persons in the Schengen Information System (SIS).
- 9 The present opinion focuses on issues that have an impact of the individuals' fundamental right to data protection. The EDPS notes that the Fundamental Rights Agency has also issued an opinion on the revised Visa Information System and its fundamental rights implications.¹¹
- 10 To facilitate the reading and the understanding of the Proposal, which amends several existing legislative texts, the present opinion will use the numbering of articles as introduced or amended by the Proposal in the existing legal texts.

2 Main recommendations

2.1 Lowering the minimum age to take fingerprints

- 11 The Proposal would amend Article 13(7)(a) of the Visa Code to lower the minimum age of the children from whom fingerprints can be taken in the visa application procedure. This age would become 6 years, instead of 12 years previously, on the basis of two studies conducted in 2013¹² and 2018¹³. These studies indicate that fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy under certain conditions.¹⁴
- 12 By lowering the age of the children from who fingerprints are taken, the Proposal aims at:
- allowing officials to verify the child's identity in the visa application procedure and enable checks at external borders,
 - strengthening the prevention and fight against children right's abuse, such as trafficking, in particular the identification/verification of identity of third country nationals who are found in Schengen territory on a situation where their rights may be or have been violated (through trafficking).
- 13 The EDPS would like to emphasize that the processing of biometric data constitutes a limitation on the fundamental rights to privacy and personal data protection. Like any interference with a fundamental right, it must comply with the criteria set out in Article 52(1) of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter")¹⁵. In addition to being provided for by law, any limitation must respect the essence of the right and, subject to the principle of proportionality, be necessary and genuinely meet objectives recognised by the Union or the need to protect the rights and freedoms of others.
- 14 Under the EU legal framework¹⁶, as well as within the framework of Modernised Convention 108¹⁷ biometric data are considered as one of the special categories of personal data¹⁸ and are subject to special protection: their processing is prohibited in principle and there are a limited number of conditions under which such processing is lawful. This specifically applies to biometric data processed for the purpose of identifying a person. The EDPS stresses that both facial images and fingerprints that would be processed pursuant to the Proposal would clearly fall within this sensitive data category.

- 15 The EU legal framework also identifies children as vulnerable individuals who deserve special protection. The General Data Protection Regulation (“GDPR”) contains a number of child-specific provisions¹⁹. In particular, Article 6(1) (f) of the GDPR provides that the processing shall be lawful if it is ‘necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child’.
- 16 The EDPS welcomes that the Proposal introduces with the new Articles 7(3) and 37(2) of Regulation 767/52008, two provisions which take the well-being of children and their specific needs into account. In particular, the new Article 37 provides that children must be informed in an age-appropriate manner, using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting procedure.
- 17 At the same time, the EDPS stresses the need to ensure that the processing of biometric data of children pursuant to the Proposal remains limited to what is strictly necessary to achieve its stated objectives. Moreover, given the particularly sensitive nature of biometrics data and the vulnerability of children, it will be necessary to provide for appropriate safeguards (see further below).
- 18 The Impact assessment mentions two main problems:
- the difficulty to unambiguously verify the identity of a child holding a visa, which is amplified by the fact that a Schengen visa can be valid for up to 5 years. This means that a child who applied with 12 years old can obtain a multiple entry visa with validity until the age of 17,
 - the estimate that between 1500 and 2000 third country national children under the age of 12 could be victim of trafficking in the Schengen area annually.²⁰
- 19 The impact assessment states that the prevention of identity fraud is raised by several consulates as the main potential benefit of the Proposal. However, it also recognises that no information is available to state the actual size of the problem.²¹ It neither explains nor provides an estimate of the scale of the problem. There are no examples of specific cases of identity fraud related to children that competent authorities have been confronted with.
- 20 As regard the number of children subject to trafficking, the impact assessment mentions that it is estimated that there could be between 1500 and 2000 third country nationals children under the age of 12 among victims of trafficking in the Schengen area each year. Although there is no information on how many of these children trafficking victims have travelled with a Schengen visa, extrapolations indicate that around 25% of them would have come through the visa process (375-500 children on a yearly basis).²²
- 21 The impact assessment refers to a Commission report on the progress made in the fight against trafficking in human beings underlying that ‘traffickers exploit loopholes in enforcement or control of legislation on work permits, visas, labour rights and working conditions’.²³ It is however unclear whether such loopholes result from mis- or non-identification of children under the age of 12, in particular those travelling with a visa to the Schengen area.
- 22 **Without further evidence supporting specifically the existence of identity fraud related to children, as well as on whether the children trafficking is rooted or**

amplified by the mis- or non-identification of children entering the EU with a visa, it is difficult to assess whether the measure proposed is appropriate and proportionate. Should further elements be provided in support of this claim, the EDPS stresses the importance of ensuring that fingerprints of the children will be used only when it is in the best interest of the child in a specific case.

23 He therefore recommends to introduce in the Proposal a specific provision on the fingerprints of children to limit their use and access for the purposes of:

- verifying the child's identity in the visa application procedure and at the external borders and,**
- contributing to the prevention and fight against children's right abuse only in a specific case.**

In particular as regards the access by law enforcement authorities, the EDPS recommends to ensure that

- such access must be necessary for the purpose of the prevention, detection or investigation of a child trafficking case,**
- access is necessary in a specific case,**
- a prior search in the relevant national databases and in the specific systems at Union level has been unsuccessful,**
- reasonable grounds exist to consider that the consultation of the VIS will substantially contribute to the prevention, detection or investigation of the child trafficking case in question and,**
- the identification is in the best interest of the child.**

2.2 Centralisation of data related to long stay visas and residence permits

24 Following the identification of an "information gap" by the High-Level Expert Group on Information Systems and Interoperability with regard to long stay visas, residence permits and residence cards²⁴, the Commission conducted a feasibility study to include in a repository documents for long-stay visas, residence and local border traffic permits. The study recommends to implement such a repository in the VIS, as this would be the most secure and cost-effective option and could be implemented with the least effort.²⁵

25 In August 2017, the Commission launched a public consultation on extending the scope of the VIS to include data on long-stay visas and residence documents. The EDPS participated in the public consultation. He stressed that no compelling evidence had yet been provided to suggest that the extension of the VIS is necessary and proportionate. Therefore, he called upon the Commission to undertake an additional reflection and evaluation of the proposed measure. He also encouraged the Commission to evaluate alternative legislative measures which could achieve the relevant objectives.²⁶

26 Under the Proposal, biometric data (including two fingerprints and a facial image) related to holders of long stay visas or resident permits would be centralised at EU level in the VIS. The two-fold problem the Proposal aims at addressing is:

- the difficulties to effectively and efficiently verify the authenticity of the documents in connection with their rightful owner as well as to fully ascertain the identity of the person holding them,**
- the lack of access to and exchange of information between Member States enabling them to properly check whether the person is not a threat to the security of the Member**

States when checking the document holders at the border crossing points and within the territory.²⁷

- 27 The EDPS recalls that the right to the protection of personal data, as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter'), also applies to third country nationals whose data are collected, stored and used by a public authority subject to European law. Under Article 52(1) of the Charter, any limitation on this right must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. This implies that the measure envisaged should be the least intrusive for the rights at stake.
- 28 According to the impact assessment the difficulty to ascertain the authenticity of a document and the legitimate relation with its holder is due to the lack of harmonisation of documents.²⁸ The impact assessment recognises that further harmonising and securing documents would help strengthen checks at external borders and in the EU territory as it would make it more difficult to forge and counterfeit the document and would thus improve the security within the EU.²⁹
- 29 The EDPS notes however that this option is not chosen since 'it would not be helpful with improving security through better information exchange', i.e. the second objective of the centralisation at EU level of data related to long stay visas and residence permits.³⁰ In particular, the impact assessment mentions that 'in order to be able to assess whether the person could pose a threat to the security of the Member States or whether he could be an identity fraudster, it is important to have access to relevant information on the previous applications made by that person and which were rejected by other Member States on grounds of national security or because of established fraudulent claims (of identity or documents)'.³¹
- 30 Under the Proposal, data related to long-stay visas and residence permits would be compared with data stored in other systems to detect whether an individual is known for a refusal of a travel authorisation, of entry or of a (short stay) visa which is based on security grounds (new Article 22b(5) of Regulation 767/2008). The EDPS recognises that this information is relevant to ensure a comprehensive assessment of the security risk of a third country national wishing to enter the EU territory.
- 31 However, the EDPS questions the need to centralise and store at EU level the data of *all* holders of a long stay visa or a residence permit to address the lack of access to and exchange of information between Member States enabling them to properly check whether the person is not a threat to security. The information stored in the VIS should be limited to individuals:
- whose data correspond to data stored in another system or where doubts remain concerning his/her identity,
 - whose request for a long stay visa and/or a residence permit has been refused because they have been considered to pose a threat to public policy, internal security or to public health or they have presented documents which were fraudulently acquired or falsified or tampered with.
- 32 The EDPS notes that by including all long stay visas and residence permits in the VIS, the Proposal would include the only category of third country nationals that are not covered by any of the EU large-scale systems.³² Given, inter alia, the envisaged interconnectivity of EU large-scale systems as set out in the Interoperability Proposal³³,

the Proposal would contribute to the establishment of an EU centralised network giving access to a considerable amount of information about every third country nationals that have crossed or are considering crossing the EU borders (i.e. millions of people) and including biometric data which are by nature very sensitive.

- 33 In particular, as regards biometric data, the EDPS notes that the issuance of long stay visas and residence permits are mainly regulated by national law. The Impact Assessment mentions that the situation as regards the collection of biometric data very much differs from one Member State to another. Not all Member States collect and store biometrics and even when they do so, a different number of fingerprints is collected with different quality criteria.³⁴ The EDPS stresses that once introduced at EU level, it would not be possible for Member States to reverse requirements for biometric data for long stay visas and residence permits through national measures alone.
- 34 **In light of the above, the EDPS recommends that the option of harmonising secure documents related to long stay visas and residence permits is further investigated and that the information stored in the VIS is limited to individuals:**
- **whose data correspond to data stored in another system or where doubts remain concerning their identity,**
 - **whose request for a long stay visa or a residence permit has been refused because they have been considered to pose a threat to public policy, internal security or to public health or they have presented documents which were fraudulently acquired or falsified or tampered with.**

2.3 Cross checking with data stored in other systems

- 35 Pursuant to the new Article 9a(3) and 22b(2) of Regulation 767/2008, the data introduced in the VIS would be compared with Europol data and data stored in:
- the VIS
 - the Schengen Information System ('SIS')
 - the Entry-Exist System ('EES')
 - the European Travel Authorisation Information System ('ETIAS')
 - the Eurodac,
 - the ECRIS-TCN system,
 - the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN) .
- 36 This comparison would be carried out for the purposes of:
- As regards short stay visas:
- examining whether the applicant fulfils the entry conditions set out in the Visa code and the Schengen Border Code i.e.:
 - o is in the possession of a valid travel document;
 - o justifies the purposes and conditions of the intended stay and has sufficient means of subsistence;
 - o is not subject to an alert in the SIS for the purposes of refusing entry.
 - assessing whether the applicant:
 - o presents a risk of illegal immigration or a risk to the security of the Member States
 - o intends to leave the territory before the expiry of the visa applied for.

- verifying that the travel document presented is not false, counterfeit or forged,
- verifying that the applicant is not considered as a threat to public policy, internal security or public health or to the international relations of any of the Member states in particular where no alert has been issued in Member State national databases for the purposes of refusing entry on the same grounds.

As regards long stay visas and residence permits:

- assessing whether the person could pose a threat to the public policy or internal security or public health of the Member States.

2.3.1 *ECRIS-TCN*

- 37 Under the new Articles 9a(3) and 22b(2) of Regulation 767/2008, the comparison of the data entered in the VIS with data recorded in the ECRIS-TCN will be carried out ‘as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned’. The EDPS wonders how it would be possible in the context of the automated querying of the ECRIS-TCN to ensure that only information on convictions related to these categories of offences will produce a hit/no hit answer (i.e. where the data stored in the VIS correspond to data stored in one or several other systems). He notes that pursuant to the proposal establishing it³⁵, the ECRIS-TCN would only contain data related to the convicted person and to the Member State holding the information on the conviction. In other words, the consultation of the ECRIS-TCN would allow to know whether the person has been convicted (or not) in a Member States but not for what offence(s).
- 38 The EDPS wishes to recall 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 has been convicted or not). As a consequence the processing of such data constitutes an interference with the fundamental rights 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. The EDPS considers that the possibility for a visa authority to know that a person has been convicted for an offence other than a terrorist or a serious criminal offence would not comply with the requirement of necessity and proportionality. Such overly broad disclosure could also harm applicants, as visa authorities might be reluctant to grant a visa to a person that has been convicted, even if not in relation to a terrorist or another serious criminal offence.
- 39 **Consequently, the EDPS recommends to include in the Proposal guarantees that only information stored in ECRIS-TCN related to terrorist and other serious criminal offences would be communicated to the central authority. One possible way could be that the central authority is not informed about the hit but a notification is automatically sent to the competent authority of the Member State that entered the data that triggered the hit. The competent authority of the Member State would then, where relevant, inform the central authority. Alternatively, the possibility to consult the ECRIS-TCN system should be deleted.**

2.3.2 *Europol data*

- 40 The EDPS stresses that the Proposal is unclear in case of a hit following a comparison of VIS data with Europol data. As regards short stay visas, the new Article 9c(8) of

Regulation 767/2008 provides that where Europol is identified as having supplied the data having triggered the hit, ‘the central authority of the responsible Member State shall consult the Europol national unit for follow-up in accordance with Regulation 2016/794 and in particular its Chapter V’. Concerning long stay visas and residence permits, the new Article 22(b)(7)(j) only provides that ‘where the hit is related to Europol data, the Europol national unit shall be informed for follow-up’.

- 41 The EDPS recalls that Europol data are collected and used for law enforcement purposes. The EDP wonders about the role and impact of data processed for law enforcement purposes in the visa issuance decision-making process. He notes that the use of the wording ‘follow-up’ is too vague and unclear. Does it imply that Europol would give a (reasoned) opinion to the issuance (or not) of the visa or that Europol would be informed about the hit(s) to use this information for its own tasks?
- 42 In the first case, the EDPS wonders to what extent, under which conditions and on the basis of which legal ground, Europol data would be taken into account in the visa issuance process and whether this would allow visa authorities to access these data. In the second case, the EDPS has repeatedly stressed that access to data stored in systems built for other purposes than law enforcement purposes should not be granted systematically but only in specific circumstances, on a case by case basis and under strict conditions. Pushing automatically information from the VIS to Europol for law enforcement purposes without any safeguards would result in circumventing the rules and conditions Europol has to comply with to access data stored in the VIS. **The EDPS recommends to clarify in the Proposal the purpose of the comparison of the VIS data with Europol data, as well as the procedure and conditions applicable as regards the outcome of such comparison.**

2.3.3 *SIS alerts*

- 43 The EDPS notes that the Proposal is unclear about the purposes of the comparison between VIS data and SIS alerts both in the context of visa issuance and in light of the SIS objectives.
- a) Comparison of Visa data with law enforcement SIS alerts for migration purposes (new Article 9a(3) of Regulation 767/2008)*
- 44 Under the new Article 9a(3) of Regulation 767/2008, the VIS would query different systems including the SIS in order to verify whether the visa applicant fulfils the entry conditions as set out in the Visa Code and the Schengen Border Code. The EDPS notes that the proposal does not specify whether the comparison would be made with all SIS alerts or only specific one(s). He stresses that contrary to the alerts related to a refusal of entry, the other SIS alerts do not refer to entry conditions but are related to law enforcement tasks (e.g. arrest an individual, locate a missing person, carry out discreet checks on suspects, etc). The EDPS considers that visa authorities shouldn’t be allowed to access these alerts unless they are legally part of the visa issuance decision-making process.
- 45 In this context, the EDPS notes that under Article 21 of the Visa Code as modified by the Proposal, the consulate would take into account alerts in respect of persons wanted for arrest or surrender purposes or wanted for arrest for extradition purposes. This would imply that such alert would be taken into account to grant a visa to an applicant (or not).

The EDPS wonders about the impact of such alerts in the visa issuance procedure taking into account the law enforcement objectives of such an alert. A consulate will be reluctant to grant a visa to individuals being subject to a European arrest warrant while it would be in the interest of law enforcement authorities that these persons get a visa to arrest them when they present themselves at the EU borders.

- 46 **The EDPS considers that the Proposal should be clarified regarding the types of SIS alerts to be taken into account in the visa issuance procedure. He recommends to ensure in the Proposal that only alerts that are legally part of the visa issuance decision-making process would produce a hit accessible by visa authorities.**

b) Use of VIS data for SIS Objectives (new Articles 9a(5) and 9c(7) and 22b(4) of Regulation 767/2008)

- 47 The new Articles 9a(5) and 22b(4) of regulation 7676/2008 provide that to support the SIS objectives, the VIS data shall be compared with data stored in the SIS to detect whether the person is:
- wanted for arrest for surrender or extradition purposes,
 - missing,
 - sought to assist with a judicial procedure or,
 - subject to discreet or specific checks.
- 48 Pursuant to the new Article 9c(7) and 22b(4) last paragraph, in case of a hit related to an aforementioned SIS alert the VIS shall send an automated notification to ‘the central authority of the Member State that launched the query to take any appropriate follow-up action’.
- 49 The EDPS understands that the aim of this provision is that law enforcement authorities are automatically informed when a person subject to a SIS alert has introduced a request in relation to a visa. However, he would like to emphasize that the wording ‘take any appropriate follow-up action’ is too vague and does not allow to determine with sufficient precision the purposes and conditions of the (further) use of the VIS data. **He therefore recommends to specify what ‘appropriate follow-up actions’ means in order to allow a proper assessment of the necessity and proportionality of the (further) use of the VIS data.**

3 Specific recommendations

3.1 Categories of VIS data compared with data recorded in other systems (new Article 9a(3) of Regulation 767/2008)

- 50 The new Article 9a(3) of Regulation 767/2008 mentions that the relevant data referred to in Article 9(4) of the same Regulation would be compared with data recorded in other systems. The EDPS considers that the wording ‘relevant’ is not precise enough. **He recommends to specify which data referred to in Article 9(4) of the Regulation 767/2008 will be compared with data recorded in other systems.** He recalls that the data to be compared must be adequate and limited to what is necessary in relation to the purpose of the comparison. For instance, there is no apparent need to compare data related to the employer of the applicant (Article 9(4)(1)) with data recorded in other systems.

3.2 Specific categories of visa applicants (new Article 9b of Regulation 767/2008)

- 51 As regards family members of EU citizens and other third country nationals enjoying the right of free movement under Union law, the new Article 9b of Regulation 767/2008 provides that the comparison of their data with data recorded in other systems shall be carried out ‘solely for the purposes of checking that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a risk to security or high epidemic risk (...)’.
- 52 The EDPS wonders about the difference between ‘factual indications’ and ‘reasonable ground based on factual indications’. He assumes that this is a misprint and **recommends to refer only to ‘reasonable grounds based on factual indications’**. Should ‘factual indications’ and ‘reasonable grounds based on factual indications’ refer to different situations, the EDPS recommends to clarify it, at least in a recital.

3.3 Definition of central authorities (new Article 9c of Regulation 767/2008)

- 53 In case there is one or several hits (i.e. where the data stored in the VIS correspond to data stored in one or several other systems), the new Article 9c of Regulation 767/2008 provides that the central authority of the Member State processing the application shall verify manually whether the identity of the applicant corresponds to the data recorded in the systems that triggered the hit. If the data correspond or a doubt remains about the identity, the central authority shall consult the central authority of the Member State(s) identified as having entered the data that triggered the hit. Where Europol is identified as having supplied the data having triggered a hit, the central authority of the responsible Member State shall consult the Europol national unit.
- 54 The EDPS notes that the Proposal does not introduce a definition of the ‘central authority’ in Regulation 767/2008 and that the new Article 9c uses various forms of this wording, i.e. the central authority of the Member State processing the application (§1), the central authority (§3), the central authorities of the other Member States (§§5-6), the central authority of the Member State that launched the query (§7), the central authority of the responsible Member State (§8). In addition, the EDPS understands that these central authorities refer in some cases to visa authorities (e.g §1) and in other cases to police authorities (e.g §7). This creates confusion. **The EDPS recommends to clarify in the new Article 9c of Regulation 767/2008 to which authority precisely each paragraph refers to.**

3.4 Use of VIS data to enter a SIS alert on missing persons (new Article 20a of Regulation 767/2008)

- 55 The new Article 20a(1) of Regulation 767/2008 provides for the possibility to use fingerprint data stored in the VIS for the purpose of entering an alert on missing persons in accordance with SIS legislation. The EDPS understands that the aim is to ‘copy’ the fingerprints stored in the VIS into the SIS when an alert about a missing person in possession of a visa is created (for instance after the disappearance of a child traveling with his family into the Schengen territory). However, the EDPS considers that the

wording of the new Article 20a(2) which stresses that '[w]here there is a hit against a SIS alert as referred to in paragraph 1' is unclear as this seems to refer to a check of fingerprint data against the SIS and not to the creation of an alert. **The EDPS calls to clarify this provision.**

3.5 Verifications in case of a hit (new Article 22b (6) and (7) of Regulation 767/2008)

56 The EDPS notes that the Proposal makes a distinction between the long stay visas and residence permits issued or extended (i) by a consular post or (ii) within the territory of a Member State.

a) Issuance or extension by a consular post

57 In case long stay visas or residence permits are issued or extended by a consular authority, the new Article 22b(6) of Regulation 767/2008 provides that the new Article 9a of Regulation 767/2008 shall apply. The EDPS notes that the reference to the new Article 9a is unclear.

58 First, the new Article 9a is under Chapter II which deals with short stay visas while the rules on long stay visas and residence permits are provided under Chapter III. Second, pursuant to the new Article 9a, other systems will be searched when 'an application file is created or a visa issued'. Would this mean that, by derogation to the new Article 22a of Regulation 767/2008, in case of long stay visas and residence permits issued or extended by a consular authority, the other systems would be searched once an application has been introduced rather than upon decision on the application? This should be clarified. Besides, the EDPS notes that the Proposal does not foresee the obligation to verify the hits resulting from the search in other systems. **He therefore recommends to clarify the reference to the new Article 9a in the new Article 22b(6) and to provide for a procedure similar to the one foreseen in the Article 9c(1) to (6) of Regulation 767/2008 to ensure that any hit related to long stay visas or residence permits issued or extended by a consular post shall be manually verified by a competent authority.**

b) Issuance or extension by an authority in the territory of a Member State

59 Where an authority in the territory of a Member State issues a residence permit or extends a long stay visa or a residence permit, that authority shall verify whether the data related to the long stay visa or the residence permit correspond to data stored in the VIS or one of the consulted systems (i.e. SIS, EES, ETIAS, ECRIS-TCN), the Europol data or the Interpol databases (new Article 22b(7)(a) of Regulation 767/2008). Where the data do not correspond and no other hits has been reported, the new Article 22b(7)(c) provides that the authority shall delete the false hit from the 'application file'. Since data related to long stay visas and residence permits are stored in an individual file (new Articles 22c to 22f of Regulation 767/2008), **the EDPS recommends replacing the wording 'application file' by 'individual file' in the new Article 22b(7)(k) of Regulation 767/2008** to avoid confusion with data related to short stay visas which are stored in an 'application file' (see Articles 8 to 14 of Regulation 767/2008).

60 Finally, the EDPS stresses that the new Article 22b(7) is unclear as regards the outcome of the verifications concluding that data related to long stay visas or residence permits correspond to data stored in other systems or where doubts remain concerning the identity of the holder of a long stay visa or a residence permit. He notes that the new Article 22b (7) only refers to situations where the hit relates to some specific SIS alerts but is silent

about hit(s) resulting from queries to other systems. In addition, the EDPS notes that the Proposal does not provide for the inclusion of the results of the verifications in the VIS as foreseen in the new Article 9c(6) of Regulation 767/2008 for short stay visas. As a result, one might wonder about the added value of the verifications for the security objectives pursued by the Proposal. **The EDPS recommends to clarify in the Proposal the outcome of the verifications concluding that data related to long stay visas or residence permit correspond to data stored in other systems or where doubts remain concerning the identity of the holder of a long stay visa or a residence permit.**

3.6 Access for law enforcement purposes (new Chapter IIIb of Regulation 767/2008)

- 61 Access of law enforcement authorities to the VIS is currently regulated in Council Decision 2008/633/JHA³⁶ which lays down the specific requirements and conditions for such access. The Proposal would repeal the Council Decision and transpose the rules governing the law enforcement access to the VIS into a new Chapter IIIb in Regulation 767/2008. This Chapter would regulate the law enforcement access to all VIS data, including those related to long stay visas and residence permits.
- 62 The EDPS notes that Recital 25 of the Proposal mentions that ‘access to VIS data for law enforcement purposes has already proven its usefulness in identifying people who died violently or for helping investigators to make substantial progress in cases related to the trafficking in human beings, terrorism or drug trafficking’. It concludes that the data in VIS related to long stays visas should therefore also be available to law enforcement authorities. However the EDPS notes that the impact assessment neither provides further indication as to how access to VIS data related to short stay visas has proven its usefulness nor explains why access to data related to long stay visas would be necessary. In addition, he notes that while the Proposal provides for law enforcement access to data related to both long stay visas and residence permits, Recital 25 only refers to data related to long stay visas.
- 63 The EDPS stresses that the mere mention of the usefulness of the access is not sufficient to justify a potentially serious limitation of the right to data protection. **Without further evidence and a detailed fact-based assessment on the need for law enforcement authorities to access data related to long stay visas and residence permits for law enforcement purposes, it is difficult to ensure that such access is appropriate and proportionate.**
- 64 Besides, the new Article 22k of Regulation 767/2008 provides that Member States have to notify eu-LISA and the Commission of their designated law enforcement authorities that are entitled to consult the VIS as well as of the designated central access points. However, while Article 3(4) of Council Decision 2008/633/JHA provides that the Commission should publish the declarations of the Member States in the Official Journal of the European Union, there is no corresponding provision in the new Article 22k. For the sake of transparency, **the EDPS recommends to add in the new Article 22k of Regulation 767/2008 an obligation for the Commission to publish the declarations of the Member States in the Official Journal of the European Union.**
- 65 The new Article 22m of Regulation 767/2008 corresponds to Article 4 of Council Decision 2008/633 which regulates the access to the VIS in case of exceptional urgency. The EDPS welcomes that §2 of this Article introduces a seven day time period for the central access point to verify whether the conditions for access are fulfilled, including whether the case of urgency actually existed. He also welcomes that §3 of the same

Article specifies that in case the verification determines that the access was not justified, all authorities that accessed the VIS data would have to erase them and inform the central access point thereof.

- 66 The EDPS considers that the new Article 22n(4) of Regulation 767/2008 is unclear. It mentions that in the event of a hit, consultation of the VIS shall give access to the data listed ‘in this paragraph’ as well as to any other data taken from the ‘individual file’. First, Article 22n(4) does not provide such list, it is therefore unclear which data are meant. Second, the use of the wording ‘individual file’ is confusing since the data related to short stay visas are stored in the VIS in an ‘application file’ (Article 8 of Regulation 767/2008) and data related to long stay visas and residence permit in an ‘individual file’ (new Article 22a of Regulation 767/2008). Finally the last sentence of the new Article 22n(4) refers to point (4)(1) of Article 9 which does not appear to exist. Moreover it seems to imply that there would be a specific verification procedure to access some categories of data stored in the VIS in addition to the procedure provided for in the new Article 22m of Regulation 767/2008. **The EDPS recommends to clarify the new Article 22n(4) of Regulation 767/2008 as regards the categories of data that will be accessible in case of a hit and the conditions of access.**
- 67 The EDPS notes that the new Article 22o of Regulation 767/2008 provides for derogations to the conditions of access to VIS data by law enforcement authorities for identification of persons who had gone missing, abducted or identified as victims of trafficking in human beings. Such access would be allowed when there are reasonable grounds to consider that the consultation of VIS data will support the identification of the person and/or contribute in investigating specific cases of human trafficking. The new Article 22o seems to distinguish between identification of a person after he/she was found, released or freed, and identification of a person, which will contribute to an investigation regarding a specific case of human trafficking. With regard to the identification of a person that will contribute to the investigation in a specific human trafficking case, the EDPS stresses that such access is clearly linked to the prevention, detection or investigation of a serious criminal offence and would thus fall under the new Article 22n of the Proposal. **The EDPS sees no reason why such access should not be subject to the conditions set out in the new Article 22n and strongly recommends to provide for justifications of the derogations.**
- 68 Finally, the EDPS recalls that the national DPAs are not responsible to check the admissibility of a request of access to the VIS. As far as the new Article 22q(3) of Regulation 767/2008 refers to the admissibility this would fall under the responsibility of the central access point. **The EDPS recommends to delete the wording ‘checking the admissibility of the request’ in the new Article 22q(3) of Regulation 767/2008.**

3.7 Statistics

- 69 Pursuant to the new Article 45a of Regulation 767/2008, duly authorised staff of the competent authorities of the Member States, the Commission, eu-LISA and the European Border and Coast Guard Agency shall have access to the data stored in VIS for the purposes of reporting and statistics without allowing for individual identification.
- 70 The EDPS understands the need to have access to data contained in the VIS for the purpose of reporting and statistics. However, it should be noted that contrary to the

wording in the new Article 45a, the combination of nationality, gender and date of birth of a person could lead to individual identification.

- 71 Therefore, **the EDPS recommends to redraft the new Article 45a of Regulation 767/2008 to recognise that the data listed under Article 45a(1) may lead to identification of individuals and therefore must be protected.**
- 72 Moreover, the EDPS observes that the new Article 45a(2) provides that eu-LISA should store the data referred to in the new Article 45a(1) in the central repository for reporting and statistics (CRRS) which will be established by the Interoperability Regulation³⁷.
- 73 The EDPS recalls that he has cautioned in its Opinion on Interoperability³⁸ against the establishment of such a statistical repository. He reiterates that such a statistical repository would impose a heavy responsibility on eu-LISA and on the EDPS, since eu-LISA would have to maintain and secure a second repository and the EDPS would have to supervise this second repository.
- 74 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.**

3.8 Use of anonymised data for testing purposes

- 75 The new Article 26(8a) of Regulation 767/2008 provides that eu-LISA should be permitted to use anonymised real personal data for testing purposes in order to diagnose and repair faults which are discovered with the Central System (a) or to test new technologies and techniques to enhance the performance of the Central System or transmission of data to it (b).
- 76 Neither the accompanying Impact Assessment nor the Explanatory Memorandum discuss the use of anonymised real personal data. In Annex 4 of the Impact Assessment, which tables the suggestions of the Regulatory Fitness and Performance Programme (REFIT), it is merely stated “*Possibility for eu-LISA to use anonymised (alphanumeric and) FP for testing purposes (similar to Article 5 Operational management of Eurodac Proposal)*” and moreover, “*Improved performance as a result of testing will benefit all end-users of the system*”.
- 77 In absence of a specific explanation of the Commission, it is not only unclear which personal data are comprised by the new Article 26(8a) of Regulation 767/2008, but also why eu-LISA needs to use real personal data to improve the VIS. However, Annex 4 of the Impact Assessment seems to suggest that some alphanumeric data and fingerprint data (abbreviated as “FP”) should be used.
- 78 The EDPS acknowledges that once alphanumeric data are truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. However, the EDPS recalls that the anonymisation of alphanumeric data constitutes further processing of personal data, which is why it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing.

- 79 Properly anonymising a dataset entails much more than simply removing obvious identifiers such as names.³⁹ For fingerprints, it should be noted that by definition, they will always refer to an identifiable person. Using synthetic test data avoids all these problems.
- 80 The EDPS also wants to draw attention that the Working Party 29 underlined in its Opinion on Anonymisation Techniques⁴⁰ that while the creation of a truly anonymous dataset is not a simple proposition in itself, even an anonymous dataset may be combined with another dataset in such a way that one or more individuals can be identified.
- 81 In addition to that, the process of rendering the production data anonymous implies that the real data have to be copied and processed to a separate technical environment from the VIS secure infrastructure by eu-LISA which creates specific security and privacy risks and which will have to be defined by a specific security risk assessment process that will address these risks.
- 82 Moreover, the EDPS recalls that fingerprint data (as well as facial images) are considered biometric data, which, by nature, are very sensitive. 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. Therefore, biometric data will always refer to an identifiable person, which is why biometric data cannot be rendered anonymous.
- 83 Against this background, Regulation 2018/1725 would fully apply to the processing of biometric data for testing purposes. Accordingly, eu-LISA would act as controller in the meaning of Article 3(8) of Regulation 2018/1725 and would have to implement appropriate technical and organisational measures to ensure the secure processing. This would impose on eu-LISA the need to establish a separate from the production, secure testing environment
- 84 The EDPS has consistently advised that whenever possible the use of production data for testing purposes should be avoided, in line with generally accepted best practices in information security⁴¹, as additional risks present themselves. Whenever possible, other means such as artificial testing data should be used instead, even when this may require additional resources.
- 85 In cases where the use of production data even after being anonymised is absolutely necessary (e.g. for specific system validation purposes), the EDPS recommends that eu-LISA performs and documents a specific risk assessment focussing on that specific use of production data. This would allow eu-LISA management to take an informed decision on these risks, taking into account other factors such as costs in terms of human resources, money or adequacy of testing.
- 86 The EDPS already stressed in its Opinion on the First reform package on the Common European Asylum System⁴², that he is not convinced that the use of real data is necessary for testing purposes. Furthermore, ISO/IEC 27002:2013⁴³ stresses that the use of real personal data poses a security risk and should altogether be avoided.
- 87 **For the aforementioned reasons, the EDPS recommends to delete the new Article 26(8a) of Regulation 767/2008.**

3.9 Data quality monitoring

- 88 The EDPS welcomes the new Article 29(2a) and the new Article 29a of Regulation 767/2008 that create a clear mandate for eu-LISA to help Member States to fulfil their obligation of ensuring data quality in the system and stress MS responsibility for including accurate and complete data in the system. The EDPS considers that the strengthened role of eu-LISA can contribute to ensuring better data quality in the system, same as clearer obligations for Member States. Ensuring that personal data in the system are correct can help to avoid taking wrongful decisions. This is of course without prejudice to the principle of data minimisation, meaning that only the data necessary for the purpose pursued should be processed.⁴⁴

3.10 Supervision of the VIS

- 89 The Regulation 767/2008 divides the responsibility for supervision between the national supervisory authorities (hereinafter “DPAs”) and the EDPS. While the DPAs are responsible to monitor the lawfulness of the processing of personal data by the Member States (Article 41 of the Regulation 767/2008), the EDPS is responsible to check that the processing of personal data by eu-LISA is in compliance with the Regulation (Article 42 of Regulation 767/2008).
- 90 To ensure a coordinated supervision of the VIS and the national systems, Article 43 of Regulation 767/2008 provides that the DPAs and the EDPS shall cooperate actively in the framework of their responsibilities, by exchanging relevant information, assisting each other in carrying out audits and inspections, examining, difficulties of interpretation or application of the Regulation 767/2008, drawing up harmonised proposals for joint solutions to any problems, promoting awareness of data protection rights, studying problems in the exercise of the rights of the data subjects. To this end, the DPAs and the EDPS shall meet at least twice a year whereas the costs and servicing of these meetings shall be for the account of the EDPS.
- 91 The EDPS notes that the modifications introduced by the Proposal in Article 43(1) of Regulation 767/2008 are confusing. While paragraph 1 of Article 43 provides for a new model of cooperation inspired from the Europol Regulation⁴⁵, paragraph 2 refers to the model envisaged in Article 62 of Regulation (EU) 2018/1725 which replaces Regulation (EC) 45/2001. The EDPS stresses that these two models differ significantly. In addition he notes that the new Article 43(1) of Regulation 767/2008 refers in an unclear way to the communication channels of the interoperability components and not to the Visa Information System.
- 92 In his opinion on the proposal for a revised Regulation 45/2001⁴⁶, the EDPS highly welcomed the approach of a single coherent model of coordinated supervision for EU large scale information systems as this will contribute to the comprehensiveness, effectiveness and coherence of data protection supervision. This will also ensure a sound environment for further development in the years to come. The EDPS understands that the objective of Regulation (EU) 2018/1725 is to use the model provided in its Article 62 for the supervision of future systems but also for existing ones. In particular Recital 78 of the Regulation (EU) 2018/1725 mentions that “[T]he Commission should make legislative proposals where appropriate with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the

coordinated supervision model of this Regulation'. **The EDPS therefore recommends that Article 43 of Regulation 767/2008 merely refers to Article 62 of Regulation (EU) 2018/1725 by mentioning only that: “The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of their respective competences, shall cooperate actively within the framework of their responsibilities and shall ensure coordinated supervision of the VIS and the national systems in accordance with Article 62 of Regulation (EU) 2018/1725”.**

4 Conclusions

- 93 The EDPS stresses that biometric data such as fingerprints are highly sensitive. Their collection and use should be subject to a strict necessity analysis before deciding to store them in a database where a large number of persons will have their personal data processed. This is even more critical when it concerns fingerprints of children who are particularly vulnerable members of our society and therefore deserve special protection.
- 94 The EDPS recognises that strengthening the prevention and fight against children right's abuses such as trafficking is of utmost importance. Nevertheless, he notes that it remains unclear whether or to what extent the child trafficking is rooted in or amplified by the mis- or non-identification of children entering the EU territory on the basis of a visa.
- 95 Should further elements be provided in support of this claim, the EDPS stresses the importance to ensure that fingerprints of the children will be used only when it is in the best interest of the child in a specific case. He therefore recommends to introduce in the Proposal a specific provision on the fingerprints of children to limit their processing to the purposes of:
- verifying the child's identity in the visa application procedure and at the external borders and,
 - contributing to the prevention and fight against children's right abuse only in a specific case.
- In particular as regards the access by law enforcement authorities, the EDPS recommends to ensure that:
- such access must be necessary for the purpose of the prevention, detection or investigation of a child trafficking case,
 - access is necessary in a specific case,
 - a prior search in the relevant national databases and in the specific systems at Union level has been unsuccessful,
 - reasonable grounds exist to consider that the consultation of the VIS will substantially contribute to the prevention, detection or investigation of the child trafficking case in question, and,
 - the identification is in the best interest of the child.
- 96 The EDPS notes that by including data on all holders of long stay visas and residence permits in the VIS, the Proposal would include the only category of third country nationals that are not currently covered by any of the EU large-scale systems in the area of freedom, security and justice. In the context of the proposed interoperability of EU large-scale systems, the Proposal would contribute to the establishment of an EU centralised network giving access to a considerable amount of information about all third-country nationals that have crossed or are considering crossing the EU borders (i.e. millions of people). Given the two-fold objective for centralising data related to long

stay visas and residence permits: (a) to ascertain the authenticity of a document and the legitimate relation with its holder and (b) to facilitate exchange of information on individuals whose visa request has been refused for security grounds, the EDPS considers that the option of harmonising secure documents related to long stay visas and residence permits should be further investigated and that the information stored in the VIS should be limited to individuals:

- whose data correspond to data stored in another system or where doubts remain concerning their identity,
- whose request for a long stay visa or a residence permit has been refused because they have been considered to pose a threat to public policy, internal security or to public health or they have presented documents which were fraudulently acquired or falsified or tampered with.

97 As regards the comparison of data stored in the VIS with data stored in other systems, the EDPS recommends to include in the Proposal guarantees that only information stored in the ECRIS-TCN related to terrorist and other serious criminal offences would be communicated to the central authority. One possible way to achieve this could be that the central authority is not informed about the hit but a notification is automatically sent to the competent authority of the Member State that entered the data that triggered the hit. The competent authority of the Member State would then, where relevant, inform the central authority. Alternatively, the possibility to consult the ECRIS-TCN system should be deleted.

98 The EDPS also recommends to clarify in the Proposal the purpose of the comparison of the VIS data with Europol data, as well as the procedure and conditions applicable as regards the outcome of such comparison. Furthermore, he considers that the Proposal should be clarified regarding the types of SIS alerts to be taken into account in the visa issuance procedure and recommends to ensure in the Proposal that only alerts that are legally part of the visa issuance decision-making process would produce a hit accessible by visa authorities.

99 Finally, beyond the general comments and key issues identified above, the EDPS has additional recommendations related to the following aspects of the Proposals:

- Categories of VIS data compared with data recorded in other systems,
- Specific categories of visa applicants,
- Definition of central authorities,
- Use of VIS data to enter a SIS alert on missing persons,
- Verifications in case of a hit,
- Access for law enforcement purposes,
- Statistics,
- Use of anonymised data for testing purposes,
- Data quality monitoring,
- Supervision of the VIS.

100 The EDPS remains available to provide further advice on the Proposal, 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 119, 4.5.2016, p. 1.
- ² OJ L 295, 21.11.2018, p. 39
- ³ OJ L 119, 4.5.2016, p. 89.
- ⁴ https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20160406_3_en
- ⁵ C (2016) 3780 final, Commission decision of 17.6.2016 setting up the High Level Expert Group on Information Systems and Interoperability.
- ⁶ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.
- ⁷ Ibidem, p. 19.
- ⁸ https://ec.europa.eu/home-affairs/news/public-consultation-lowering-fingerprinting-age-children-visa-procedure-12-years-6-years_en.
- ⁹ https://ec.europa.eu/home-affairs/content/consultation-extending-scope-visa-information-system-vis-include-data-long-stay-visas-and_en.
- ¹⁰ EDPS response to the Commission public consultation on extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents, available at: https://edps.europa.eu/sites/edp/files/publication/18-02-09_formal_comments_vis_consultation_long_stay_visas_residence_documents_en.pdf and EDPS formal comments in response to the Commission public consultation on lowering the fingerprinting age for children in the visa procedure from 12 to 6 years old, available at: https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_en.pdf.
- ¹¹ Opinion of the Fundamental Right Agency on the revised Visa Information System and its fundamental rights implications, 30 August 2018, available at: <http://fra.europa.eu/en/opinion/2018/visa-system>.
- ¹² ‘Fingerprint Recognition for Children, technical report by the Joint Research Centre, 2013, available at <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf>
- ¹³ ‘Automated fingerprint recognition : from children to elderly ageing and age effects’, technical report by the Joint Research Centre, 2018, available at <https://ec.europa.eu/jrc/en/publication/automatic-fingerprint-recognition-children-elderly-ageing-and-age-effects>
- ¹⁴ Recital 8 of the Proposal.
- ¹⁵ Article 2 of the Treaty on the European Union (“TEU”) states that “*The Union is based on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*”. In addition, Article 6(1) TEU recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg on 12 December 2007, which has the same legal value as the treaties, and Article 6(3) TEU states that “*fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union’s law*”.
- ¹⁶ See Article 9 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, 4.5.2016, p. 1–88 and Article 10 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.
- ¹⁷ Article 6 of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted on 17-18 May 2018
- ¹⁸ The General Data Protection Regulation refers to sensitive personal data as “*special categories of personal data*” (see Article 9 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88)
- ¹⁹ See Recitals 38, 58, 65, 71, 75 and Articles 6(1)(f), 8, 12, 40, 57 of the General data protection Regulation
- ²⁰ Impact assessment, p.14.
- ²¹ Impact assessment, annex 8, p. 104
- ²² Impact assessment, p.14 and 105.

-
- ²³ Commission report to the European Parliament and the Council on the progress made in the fight against trafficking in human beings, SWD (2016) 159 final, p.16.
- ²⁴ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.
- ²⁵ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/201709_ibm_feasibility_study_final_report_en.pdf.
- ²⁶ https://edps.europa.eu/sites/edp/files/publication/18-02-09_formal_comments_vis_consultation_long_stay_visas_residence_documents_en.pdf.
- ²⁷ See impact assessment p. 17-18 and explanatory memorandum p. 7-8.
- ²⁸ Impact assessment, p. 18,
- ²⁹ Impact assessment, p. 45 and 59.
- ³⁰ Impact assessment p. 45.
- ³¹ Impact assessment p. 19.
- ³² Explanatory memorandum p. 7.
- ³³ COM(2017) 794 final, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration).
- ³⁴ See Annex 10 of the impact assessment, p.119.
- ³⁵ Proposal for a Regulation of the European Parliament and of the Council 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.
- ³⁶ 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
- ³⁷ COM(2017) 793 final, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.
- ³⁸ https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf.
- ³⁹ Article 29 Working Party [Opinion 05/2014 on Anonymisation Techniques](#), WP216. While that documents analyses anonymisation techniques in the framework of the old data protection directive 95/46, its reasoning remains valid under GDPR.
- ⁴⁰ Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, WP216.
- ⁴¹ ISO/IEC 27002:2013, section 14.3.
- ⁴² https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf.
- ⁴³ Cf. Section 14.3 of ISO/IEC 27002:2013, Guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).
- ⁴⁴ Art. 5(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), JOCE, L 119/1, 4 May 2016
- ⁴⁵ 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, 24.05.2016.
- ⁴⁶ Opinion 5/2017 "Upgrading data protection rules for EU institutions and bodies, EDPS opinion on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 15 March 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf.