

FREEDOMS



Fundamental rights and the interoperability of EU information systems: borders and security



FRA

EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS



This report addresses matters related to the right to respect for private and family life (Article 7), to the protection of personal data (Article 8), and to an effective remedy (Article 47), as well as to the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), liberty and security of person (Article 6), integrity of the person (Article 3), the right to asylum (Article 18), prohibition of collective expulsion (Article 19), rights of the child (Article 24) and equality before the law (Articles 20). These fall under Titles I 'Dignity', II 'Freedoms', III 'Equality' and VI 'Justice' of the Charter of Fundamental Rights of the European Union.

**Europe Direct is a service to help you find answers
to your questions about the European Union.**

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Photo (cover & inside): © Shutterstock

More information on the European Union is available on the Internet (<http://europa.eu>).

FRA – European Union Agency for Fundamental Rights
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu – info@fra.europa.eu

Luxembourg: Publications Office of the European Union, 2017

Paper: 978-92-9491-722-5 10.2811/178106 TK-01-17-325-EN-C
PDF: 978-92-9491-721-8 10.2811/516971 TK-01-17-325-EN-N

© European Union Agency for Fundamental Rights, 2017

The manuscript for this publication was completed in May 2017.

Reproduction is authorised, provided the source is acknowledged.

Printed in Italy

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

Fundamental rights and the interoperability of EU information systems: borders and security

Foreword

Interoperability between EU information systems in the areas of borders and security aims to provide fast and easy access to information about persons crossing the borders to enter the European Union (EU). Currently, various proposals on EU-level information systems mention interoperability. In a nutshell, these systems would include information about all third-country nationals – whether applying for asylum or just arriving in the EU for a short stay.

When used to obtain information about individuals entering the EU, this entails both opportunities and risks from a fundamental rights perspective. Interoperability does not intrinsically violate fundamental rights. However, adequate safeguards and mechanisms to protect the rights set out in the EU Charter of Fundamental Rights are essential. Interoperability implicates a number of such rights – especially to respect for private life and the protection of personal data. In the areas of borders and security, it can also affect many other rights, such as the rights of the child, the right to asylum, liberty and security of person and the right to an effective remedy. Moreover, the actual broader availability of data can in itself have additional implications – both positive and negative.

This publication was originally prepared to support discussions in the high-level expert group on information systems and interoperability, tasked with elaborating the legal, technical and operational aspects of options for achieving interoperability of information systems. Convened by the European Commission, the discussions brought together relevant experts nominated by EU Member States, Schengen associated countries, and EU agencies and bodies.

FRA aims to provide solutions to existing fundamental rights challenges – and to prevent new ones from emerging. This report is an important element in that work.

Michael O’Flaherty
Director

Contents

FOREWORD	3
EXECUTIVE SUMMARY	7
INTRODUCTION	11
What is interoperability?	12
IT-systems that could become interoperable	15
1 DATA PROTECTION: DATA MINIMISATION, PURPOSE LIMITATION AND DATA RETENTION	19
1.1. Biometric data	20
1.2. Data minimisation	21
1.3. Purpose limitation	21
1.4. Storage limitation	23
Conclusions	24
2 FUNDAMENTAL RIGHTS RISKS OF UNLAWFUL ACCESS OR USE OF PERSONAL DATA	25
2.1. Indirect access	26
2.2. Access by private persons	26
2.3. Increased number of access points	26
2.4. Sharing with third countries	27
Conclusions	28
3 FUNDAMENTAL RIGHTS CONSEQUENCES OF TAKING DECISIONS ON THE BASIS OF LOW QUALITY OR UNLAWFULLY STORED DATA	29
3.1. Alphanumeric data	30
3.2. Biometric data	31
3.3. The right to rebut a false assumption	32
3.4. Right to access own data and have incorrect data rectified	33
Conclusions	34
4 RIGHTS OF THE CHILD	35
4.1. Amplified effects of interoperability on children	35
4.2. Interoperability as a tool for child protection	36
Conclusions	38
5 INTERNATIONAL PROTECTION	39
Conclusions	40
6 RISK OF DISPROPORTIONATE EFFECTS ON THE RIGHTS OF MIGRANTS IN AN IRREGULAR SITUATION	41
Conclusions	41
7 RISK OF UNLAWFUL PROFILING WHEN UNDERTAKING RISK ASSESSMENT	43
Conclusions	44
REFERENCES	45
ANNEX: RESEARCH METHODOLOGY	49

Executive summary

Interoperability between EU information systems in the areas of borders and security aims to assist in decision making by providing a more complete picture about a person. Such information systems cover mainly non-EU citizens, including short-term travellers, asylum seekers, and third-country nationals with criminal records.

Depending on the technical solution chosen, interoperability can create new fundamental rights challenges or amplify those already present in existing systems. At the same time, interoperability can provide new opportunities to offer more robust and timely protection – for example, in the case of missing children.

Due to the underlying aim of interoperability – providing easy and quick access to information about third-country nationals – a number of the challenges are linked to the right to private life (Article 7 of the EU Charter of Fundamental Rights (the Charter)) and the protection of personal data (Article 8 of the Charter). Furthermore, the actual broader availability of data can in itself have additional implications – positive or negative – on, for instance, the right to an effective remedy (Article 47) or the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), liberty and security of person (Article 6), integrity of the person (Article 3), the right to asylum (Article 18) and prohibition of collective expulsion (Article 19), rights of the child (Article 24) and equality before the law (Articles 20).

Protection of personal data

According to Article 8 (1) of the Charter, everyone has the right to the protection of their personal data. Article 7 stipulates the right to respect for private life. Any interoperable solution or solutions selected for the EU information systems will need to be designed in a manner that does not unduly affect core data protection principles. Data protection by design and by default (commonly referred to as ‘privacy by design’) is often highlighted as a precondition for establishing interoperability in line with core data protection principles.

Alphanumerical data can be unreliable for establishing the identity of a person, whereas the use of biometric data makes the matching significantly more reliable. Interoperability needs to respect the special sensitivity of biometric data, which require additional safeguards to be considered when such data are processed.

Interoperability should not lead to the processing of more – biometric or alphanumerical – data than

necessary for the existing purposes under the individual legal instruments. Technical solutions chosen must limit access only for authorised purposes and to authorised staff and must provide for automated deletion of data to comply with legally set retention times. The biometric matching service and the single search interface should not be programmed to actually store data, but only to match it.

If interoperability solutions envisage the possibility to show ‘flagged’ hits, which would inform an officer about the existence of additional data that he or she is not authorised to access, adjustments will be necessary to the legal instruments establishing the different information systems. The knowledge of the existence of additional information about the person, such as an entry in ECRIS or SIS II, possibly under another name, may support the identification of the person and influence the decision-making.

Interoperable databases may be highly attractive for those trying to access personal data by illegal means, not only organised crime groups but potentially also hackers linked to foreign states. One of the pillars of any interoperable solution must therefore be strong data security measures. Particularly mobile devices would need to be secured against unauthorised access. In instances when officers may request indirect access to information stored, effective verification procedures are necessary to determine if the requesting person is authorised to receive the information.

Because interoperability will make access to data easier, it increases the chances that data are unlawfully shared with third countries. This risk would be exacerbated if ‘flagged’ hits would be accessed, as a hit in Eurodac would indicate that the person is an asylum seeker. Safeguards would need to be in place to ensure that the rules on sharing of data with third countries as laid down in the individual legal instruments are adhered to also in case of interoperability.

Right to an effective remedy

Data stored in information systems may not always be accurate and therefore not always reliable. Interoperability provides the authorities with increased opportunity to become aware of inaccuracies. Authorities should, therefore, develop standardised procedures for automatic verification with data stored in other IT systems and correct inaccurate data immediately. On the other hand, if the personal data which are re-used are incorrect, interoperability may possibly lead to inaccurate information being taken over from one system to

another. Mistakes are not necessarily due to the accuracy of the data, but also to administrative errors – for instance, if the biometric data are attached to the alphanumeric data of another person.

Due to the high degree of credibility attached to biometric data as well as the technical complexity of processing them, it is difficult to rebut errors based on biometrics. To give effect to the right to rebut a false assumption based on biometric data, the authorities would need to be ready to address plausible arguments presented by the data subject.

Complying with the duty to inform may be additionally complicated in a situation of interoperability. The officer accessing the databases would first need to be clearly aware of which database he or she is consulting, which may not be obvious when consulting several information systems. Not ensuring the right to information may make it impossible for the person concerned to exercise his or her right to access own data and have it rectified where necessary, which is a recognised fundamental right in Article 8(2) of the Charter.

Rights of the child

Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions taken in relation to children by public authorities and private actors. Interoperability may magnify some pre-existing risks in the case of children, particularly as the child had no say in the parents' decision to migrate.

The physical development of the child may reduce the reliability of matches based on biometric data, particularly after a longer period of time. Matches based on fingerprints older than five years, or on a facial image, should therefore always be subject to further checks and verified against other available data.

Information on criminal records may have a disproportionate impact on children – for example, when they relate to immigration offences for which the children cannot be held responsible. In light of the vulnerability of children, consideration should be given to either excluding information on criminal records of children from the scope of the interoperable solutions altogether, or to limiting the availability of this information to very serious crimes committed by children.

Interoperability can support the detection of missing children or children subject to trafficking in human beings, and facilitate a targeted response. This requires the systematic recording of missing children in SIS II, an additional focus on child protection in the individual IT systems, particularly in Eurodac, as well as functioning referral mechanisms and tailor-made training of

practitioners who may encounter children in need of protection.

International protection

Under EU law, Article 18 of the Charter protects the right to asylum. Effective access to international protection also forms the basis for the protection from *refoulement*, which is reflected in Article 19 of the Charter.

Through interoperability, identity fraud will be more easily identified. However, the use of false documents should not have an undue impact on decisions to grant international protection, as many seek to hide their identity when fleeing their country of origin to protect themselves, while others may be physically unable to obtain the documents necessary for legal entry (such as a passport and visa) when escaping from a conflict zone. Moreover, information originating from third countries that may be consulted through interoperability should not be taken at face value; for instance, oppressive regimes may include information about opponents in the Interpol database SLTD (Stolen and Lost Travel Documents) to prevent them from leaving the country.

Interoperability may have beneficial effects for persons seeking international protection. By ensuring that the status as an applicant for international protection is visible also when consulting other systems, it would reduce the risk of apprehension, detention or return, and also contribute to respect for the principle of non-*refoulement*. Past records in other systems may also help establish the identity of an undocumented person forced to flee persecution or other risk of harm.

Rights of migrants in an irregular situation

Making the EU's information systems interoperable can contribute to more efficient immigration law enforcement, as a number of systems can simultaneously be accessed to determine if a person who has been stopped has the right to stay. Certain enforcement measures have a disproportionate impact on their ability to enjoy basic rights protected by the Charter, such as the right to education (Article 14), the right to health care (Article 35) and the right to an effective remedy (Article 47), which must be provided to everyone, without discrimination.

Due to the risk of apprehension irregular migrants become afraid of approaching health services or send their children to schools. Victims of crime may be reluctant to approach the police for fear that this would lead to their removal, which puts them at risk of further victimisation and allows perpetrators to go unpunished.



FRA's guidelines on the rights-compliant apprehension of migrants in an irregular situation (2014) recommends amongst others that there should be possibilities for victims and witnesses to report crime without fear of being apprehended, which is of particularly importance as interoperability supports the security agenda.

Risk of unlawful profiling

The data contained in information systems can be used for risk assessment or profiling. The use of sensitive data for profiling is exceptionally permitted where it is necessary for reasons of substantial public interest, on the basis of EU or Member State law. Even where the profiling is based on public interest stipulated in law, it will still be considered unlawful where it is discriminatory in nature, either directly or indirectly. In the words of the Racial Equality Directive (2000/43/EC), discrimination occurs 'where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin.' Article 11 (3) of the Data Protection Directive (EU) 2016/680 explicitly prohibits any profiling that results in discrimination on the basis of sensitive data. Automated risk assessment or profiling would, therefore, have to be based on algorithms that are not primarily or solely determined by personal characteristics that reveal sensitive information, such as, race, ethnicity, health, sexual orientation, and religious beliefs. By increasing the availability of this information contained in individual databases, interoperability may increase the risk of discriminatory profiling.

At the same time, access to additional information due to interoperability may help reduce the likelihood of discriminatory risk assessment based on sensitive personal data. This is because it would allow conducting more focused searches based on a combination of non-sensitive criteria instead of relying on a limited number of sensitive categories.

Conclusion

Interoperability involves both risks and opportunities for fundamental rights. Receiving the full picture about a person contributes to better decision-making. To this end, safeguards need to be in place to ensure the quality of the information stored about the person and the purpose of the data processing. Such safeguards should prevent unauthorised access and unlawful sharing of information with third parties. To ensure the right to an effective remedy, practical possibilities to rebut a false assumption by the authorities and to have inaccurate data corrected need to be in place.

Interoperability can support the detection of missing children or children subject to trafficking in human beings, and facilitate a targeted response. This requires the systematic recording of missing children in SIS II, and an additional focus on child protection in the individual IT systems. Interoperability can also contribute to respect for the principle of non-*refoulement* by ensuring that the status as an applicant for international protection is also visible when consulting other information systems. Risks for discriminatory profiling may be reduced if a combination of non-sensitive criteria is used instead of relying on a limited number of sensitive categories.

Introduction

When authorities take immigration and security-related decisions concerning an individual, they first need to establish the person's identity. They do this increasingly by relying on large-scale databases, so-called information technology systems (IT-systems), where personal data of a large number of people are stored. According to current plans, in a few years, the personal data of more or less all third-country nationals coming for a short stay to the European Union (EU) would be captured in one or more information systems set up by the EU. In contrast, EU nationals remain mainly listed in national databases and EU systems only cover specific categories of them.

Biometric data are increasingly used to identify a person. Biometrics are unique to the person in question and considered as the most reliable method to identify a person. In the EU, fingerprints and facial images are the most commonly used biometric identifiers. The EU Agency for Fundamental Rights (FRA) has been analysing the fundamental rights implications of processing biometric data in large-scale EU IT-systems since 2015, when the agency started to work on a dedicated project on biometrics (see FRA Activity Box).¹ This paper builds on FRA's work within that project, particularly on how the fundamental rights of an individual whose data are included in an IT-system may be affected.

Authorities see easy and quick access to relevant personal data about third-country nationals as crucial to preventing security threats, as well as to take immigration-related decisions more efficiently. To this end, the European Commission has suggested that existing IT-systems, which currently operate in silos, would need to "speak to each other". In other words, interoperability is the ability of different IT-systems to communicate, exchange data and use the information that has been exchanged. In the asylum, borders and security context, it means that when consulting an IT-system, more information about a person becomes available in one search, rather than having to undertake multiple searches in different systems. To support this aim, in its Communication in April 2016, the European Commission proposed different options on how such interoperability among IT-systems could be achieved.² These options are described in the section on '[What is interoperability?](#)'.

In June 2016, under the Dutch EU Presidency, the Council produced a 'Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area'.³ To assess the technical and legal aspects, including its fundamental rights implications, the European Commission convened a High Level Expert Group on information

FRA ACTIVITY

Biometric data in large EU IT-systems in the areas of borders, visa and asylum – fundamental rights implications (FRA biometrics project)

The project on biometrics in large-scale EU databases analyses the fundamental rights implications of collecting, storing and using biometric and other data in EU IT-systems in the field of visas, borders and asylum. It examines both positive and negative fundamental rights implications of storing biometric and other data in Eurodac, SIS II (Schengen Information System) and VIS (Visa Information System). The research comprises a mapping of relevant practices and procedures in all EU Member States, carried out by Franet, as well as fieldwork research in six selected EU Member States based on the different migration challenges they face. Eticas Research and Consulting, and the Spanish Research Council (CSIC), Department of Demography, carried out the fieldwork research on behalf of FRA.

The fieldwork research included in-depth interviews carried out with public officials, asylum seekers and migrants, as well as experts (total 286 interviews), in addition to three small-scale surveys carried out with border guards (160 respondents) and staff processing visa applications at embassies and external service providers (132 respondents) and with visa applicants (584 respondents). The survey among border guards was conducted at border crossing points in six EU Member States, including Zeebrugge port in Belgium, the airports Frankfurt in Germany, Barajas in Spain, Fiumicino in Italy and Arlanda in Sweden, as well as the border crossing point Terespol in Poland. The surveys among staff working at consulates and visa applicants were conducted in four countries including Algeria, Nigeria, Thailand and Ukraine.

This paper draws on findings of this project (for more details, see the [Annex](#)).

¹ FRA (European Union Agency for Fundamental Rights) (2015a).

² European Commission (2016), *Stronger and smarter information systems for borders and security*, COM(2016) 205 final, Brussels, 6 April 2016.

³ Council of the European Union (2016b).

systems and interoperability, as envisaged by its April 2016 Communication, in which EU Member State officials and representatives of relevant EU institutions and agencies, including FRA, participated.⁴ More recent legislative proposals concerning information systems, which the European Commission put forward, expressly refer to the interoperability of IT-systems. This paper highlights the fundamental rights implications of interoperability between IT-systems and has been drafted to support the discussions on this topic within the EU.

Having more information about a person available at once entails both risks and opportunities for the respect of that person's fundamental rights. Depending on the particular technical solution(s) chosen, interoperability can create additional challenges or amplify those pertinent to the existing systems. At the same time, interoperability can provide new opportunities to offer more robust and timely protection – for example, for missing children. If sufficient evidence supports the premise that interoperability can prevent the loss of civilian lives through, for example, a terrorist attack, one could argue that Member States have a duty to use the information available to them more effectively. The European Court of Human Rights (ECtHR) has stated that the right to life in Article 2 of the European Convention of Human Rights (ECHR) implies a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk, if they knew or ought to have known of the existence of an immediate risk.⁵ So far, however, supporting evidence that interoperability can prevent loss of life is scarce. In the context of terrorist prevention, for instance, the United Kingdom says that access to large volumes of data through bulk interception is the only way for security and intelligence agencies to gain insight into particular areas and threats.⁶

Due to the underlying aim of interoperability – providing easy and quick access to information about third-country nationals – a number of the fundamental rights challenges are linked to the right to respect for private life (Article 7 of the Charter of Fundamental Rights of the EU (the Charter)) and the right to protection of personal data (Article 8 of the Charter). Furthermore, the absence of adequate safeguards and mechanisms to ensure a high level of data protection can have adverse effects on a number of other Charter rights, such as the right to good administration (Article 41), the right to an effective remedy (Article 47), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), the right to liberty and security of

a person (Article 6) and the right to the integrity of the person (Article 3). Finally, the actual broader availability of data can have additional implications – both positive and negative – in the field of asylum (Articles 18 and 19), the right of the child (Article 24) or the right to equality before the law (Articles 20).

Interoperability is part of a trend towards an increased use of technology by border, immigration and law enforcement authorities. Academic writers have argued that the increasing collection and storage of data is likely to affect societies and individuals in multiple ways. This is particularly the case when biometric data are processed.⁷ According to some experts, curtailing privacy by processing large amounts of personal data, including biometric data, may affect democracy and society since privacy is a value inherent to a liberal democratic and pluralist society, and a cornerstone for the enjoyment of human and civil rights.⁸

What is interoperability?

The Digital Agenda for Europe (2010)⁹ identifies improved interoperability as one of the key aspects promoting growth. Interoperability allows administrative entities to exchange electronically meaningful information in ways that all parties understand. The European Commission has supported programmes to develop, promote and use interoperability solutions in the public sector in the EU.¹⁰ It has also stated that interoperability should be taken into account when legislative instruments are drafted.¹¹

The 2016 European Commission Communication on stronger and smarter information systems for borders and security builds on synergies identified in the

4 High level Expert Group on Information Systems and Interoperability, *Register of Commission Expert Groups*.
5 European Court of Human Rights (ECtHR), *Osman v United Kingdom*, No. 87/1997/871/1083, 28 October 1998, para. 116.
6 See, for example, Anderson, D.Q.C. (2016).

7 Alterman, A. (2001), p. 144.
8 Hallinan, D. (2015), pp. 268-270; Raab C. (2015), pp. 259-268; Goncalves, M. E. and Gameiro, M. I. (2014), p. 29.
9 European Commission (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, COM(2010) 245 final/2, Brussels, 26 August 2010.
10 European Commission (2010), *Towards interoperability for European public services*, COM(2010) 744 final, Brussels, 16 December 2010; European Commission (2015), *A digital Single Market Strategy for Europe*, COM(2015) 192 final, Brussels, 6 May 2015; Decision No. 922/2009/EC of the European Parliament and of the Council of September 2009 on interoperability solutions for European public administrations (ISA); Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA² programme) as a means of modernising the public sector; European Commission (2017), *European Interoperability Framework-Implementation Strategy*, COM(2017) 134 final, Brussels, 23 March 2017.
11 European Commission (2017), COM(2017) 134 final, Brussels, 23 March 2017.

European Agendas for Security¹² and Migration.¹³ It considers interoperability as a means to enhance both border management and external security. The current systems are described as fragmented due to different institutional, legal and policy contexts across the EU and its Member States. Inconsistencies and diverging access cause difficulties in recognising connections between data sets. The Commission Communication defines interoperability as the ability of information systems to exchange data and to enable the sharing and access to information. The trust in IT-systems and the information they hold explains why the Communication also underlines the importance of the quality of the data. It identified four options to achieve interoperability:

- a single search interface;
- a biometric matching service;
- a common repository of data;
- interconnectivity.

The following sections further explain these four options to achieve interoperability.¹⁴

A single-search interface

A single-search interface (Figure 1), or a European search portal, aims to query several information systems simultaneously and produce combined results on one single screen.

A single search interface could be added to the search functions of the current IT-systems.

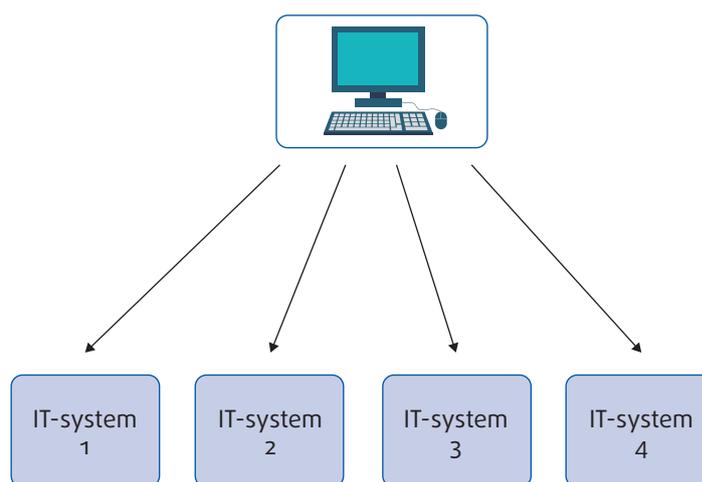
The single search interface can be accessed with alpha-numerical data or it can be used in combination with a biometric matching service as described in the following sub-section.

Most EU Member States use single search interfaces for simultaneously accessing separately maintained national databases. For instance, Germany uses the police database INPOL to access separate national databases. Some Member States have included national copies of SIS II (Schengen Information System) in the national search interface, whereas others can access the central SIS II through their national search interface. It would also be technically possible for Member States to set up a single search interface capable of accessing both national and European databases at the same time.

A shared biometric matching service

A shared biometric matching service (Figure 2) uses the same biometric identifier to search the various information systems. It enables the identification of a person through the biometric data stored in an IT-system. A biometric matching service would increase the reliability of the identification of a person across many IT-systems, without having to rely solely on alphanumeric data,

Figure 1: Single search interface



Source: FRA, 2017

¹² European Commission (2015), The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28 April 2015.

¹³ European Commission (2015), A European Agenda on Migration, COM(2015) 240 final, Brussels, 13 May 2015.

¹⁴ European Commission (2016), COM(2016) 205 final, Brussels, 6 April 2016.

which may be incorrect or may result in many matches with persons who have the same name.

A biometric matching service would use common biometric identifiers. In the EU, these would typically be fingerprints and/or facial images to check against multiple databases if there is a match with the biometric feature stored in an IT-system. A shared biometric matching service could be attached to one of the other interoperability options, for example, single search interface, a common repository, or interconnected IT-systems, and would look for a biometric match within the different IT-systems covered, sending a response based on whether a match has been found ('hit/no hit').

At present, biometric checks can only take place against one single database at a time, such as Eurodac or VIS, through the automated fingerprint identification system (AFIS).

A common repository of data

The purpose of a common repository of data (Figure 3) is to make available certain core personal data from different IT-systems by using the biometrics matching service to identify the person. A common repository would make it possible to retrieve all stored data about a person, even if he or she appears under different identities in various IT-systems. It would link different identities in various IT-systems through biometrics

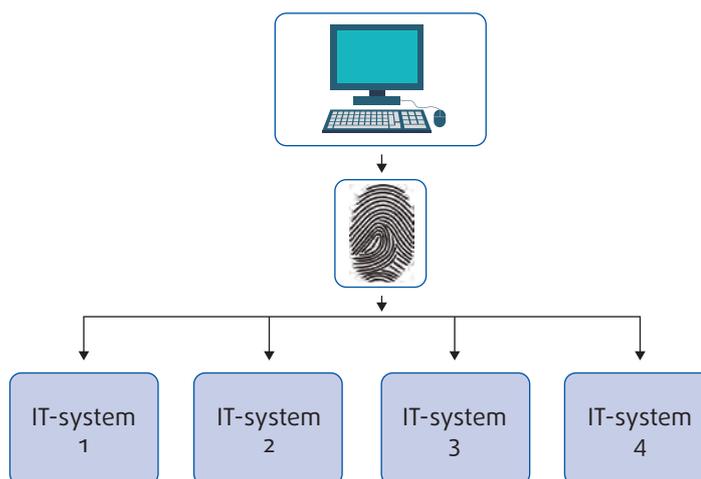
and present these links in "views".¹⁵ The data shown in such "views" would include alphanumeric data, such as name, date of birth and gender, linked to various identities of the same person. These "views" could be stored and maintained over time to keep up the connections to the source data. These maintained "views" would need to be 'synchronised' regularly to capture changes entered into the IT-systems after the view is created.

The "views" could only show "hits" which the viewer is authorised to consult according to the respective legal instruments. Alternatively, they could be programmed in a manner that also enables the officer querying the systems to see if there are other hits, the content of which he or she is not allowed to view – so-called "flagged hits".

Interconnectivity of information systems

The interconnectivity of information systems implies that data registered in one system are automatically consulted by other systems; this represents another option for achieving interoperability. To this end, the IT-systems are technically connected. The systems need to be technically compatible and the data elements stored need to have a very similar interpretation. As the discussions in the High Level Expert Group have so far not focused much on interconnectivity, this paper will not discuss this option.

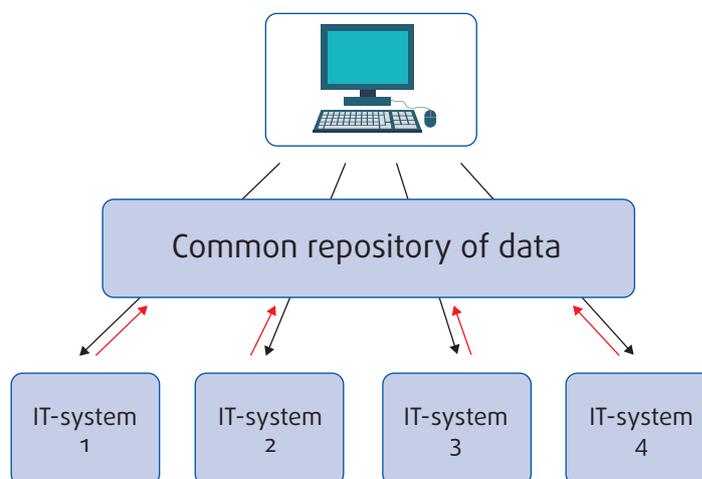
Figure 2: Biometric matching service



Source: FRA, 2017

¹⁵ Wikipedia, [View \(SQL\)](#).

Figure 3: A common repository of data



Source: FRA, 2017

IT-systems that could become interoperable

Discussions on interoperability cover both existing and proposed EU IT-systems, as well as Europol databases and the Interpol databases SLTD (Stolen and Lost Travel Documents) and TDAWN (Interpol Travel Documents Associated with Notices database). Interoperability could also possibly include national IT-systems.

At the EU level, existing IT-systems are the Schengen Information System (SIS II),¹⁶ Eurodac (European

Dactyloscopy)¹⁷ and the Visa Information System (VIS).¹⁸ New proposed systems are the Entry-Exit System (EES)¹⁹ and the European Travel Information and Authorisation System (ETIAS).²⁰ Although ECRIS (European Criminal

¹⁶ Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2006 L 381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2007 L205/63 (SIS II).

¹⁷ Council Regulation (EC) No. 603/2013 of 26 June 2013 on establishment of Eurodac (recast) OJ 2013 L 180/1; Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ 2009 L 93/33; European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)*, COM(2016) 272 final, Brussels, 2 May 2016.

¹⁸ Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ 2008 L 218/60 (VIS regulation).

¹⁹ European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No. 767/2008 and Regulation (EU) No 1077/2011*, COM(2016) 194 final, Brussels, 6 April 2016.

²⁰ European Commission (2016), *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, Brussels 16 November 2016, p. 15.

Records Information System) already exists as a network of national criminal registers,²¹ the European Commission suggested a specific centralised database holding only the criminal records of third-country nationals. A revised proposal is expected in 2017. References to ECRIS in the present document refer to its present functionalities and not possible future ones.

Europol databases (such as the Europol Information System, EIS) are not included among the central EU IT-systems. Access to the Europol Information System (EIS) from national single-search interfaces is being piloted through the web service QUEST (Querying Europol Systems).²²

National IT-systems can be either purely national or data can be processed in a national system but regulated by EU-law, such as the Passenger Name Record (PNR)²³ or the Advanced Passenger Information (API).²⁴ Even if purely national, EU Member States may exchange information between each other by exchange mechanisms, such as Prüm.²⁵

Table 1 shows the IT-systems that are considered in the discussions on interoperability. As the specifics of a proposal on ECRIS cannot be assessed yet, ECRIS is covered neither in this table nor in the following ones.

The EU IT-systems have been or are being set up for different purposes. These include the application of the Dublin Regulation (Eurodac), police and border checks (SIS II), visa processing and border checks of visa holders (VIS), pre-border checks (ETIAS), registration of entry and exit (EES), and exchange of information on criminal convictions (ECRIS). These systems also have additional purposes, such as access by law enforcement to fight serious crime and terrorism or immigration law enforcement purposes.

Increasingly more categories of third-country nationals are included in the IT-systems – visa applicants, irregular migrants, travellers coming for a short-term visit, without or with a visa. The only exception are third-country nationals staying on a long-term basis, as there is no

dedicated EU-wide IT-system holding residence applications. Through interoperability, EU Member States would in one search potentially access all data stored on a person in the EU IT-systems. These would cover all short-term travellers, asylum applicants and in the future third-country nationals with criminal records.

Recent legal instruments proposed by the European Commission consider in one way or the other the option of interoperability. The proposal for a revision of Eurodac,²⁶ for example, refers to future interoperability with SIS II and VIS, where necessary and proportionate. When presenting the SIS II proposals on police and judicial cooperation,²⁷ borders checks²⁸ and return²⁹ on December 2016 the European Commission stated that it may consider revising the proposals to further improve their interoperability with other IT-systems. The European Commission report on the evaluation of VIS³⁰ sees a potential for interoperability with Eurodac, EES, SIS II, and the SLTD. The ETIAS proposal envisages interoperability with EES, VIS, Europol, SIS II, Eurodac and ECRIS and a common repository of data of third-country nationals shared between ETIAS and EES. There is a need for a compatibility assessment between the respective purposes of the systems before considering access to and the use of data collected and processed in other systems, as underlined by the European Data Protection Supervisor (EDPS).³¹ This paper examines the fundamental rights implications of interoperability. Besides the various elements of the right to the protection of personal data, it looks at other fundamental rights potentially affected, such as the rights of the child

21 Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ 2009 L 93/33.
22 Council of the European Union (2016b).
23 Directive 2016/681 of the European Parliament and of the Council of 7 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016, L 119/132.
24 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 2004, L 261/24 (API Directive).
25 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, OJ 2008 L 210/1.

26 European Commission (2016), COM (2016) 272 final, Brussels, 2 May 2016.

27 European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU*, COM(2016) 883 final, Brussels, 21 December 2016.

28 European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006*, COM(2016) 882 final, Brussels, 21 December 2016.

29 European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third country Nationals*, COM(2016) 881 final, Brussels, 21 December 2016.

30 European Commission (2016), *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, COM(2016) 655 final, Brussels, 14 October 2016, p. 9.

31 European Data Protection Supervisor (EDPS) (2017).



Table 1: EU IT-systems possibly envisaged for interoperability and persons included

	Eurodac	VIS	SIS II: police	SIS II: immigration control	EES proposal	ETIAS proposal
Persons included	Applicants for international protection, refugees and irregular migrants, according to Eurodac proposal	Visa applicants and sponsors	Missing or wanted persons	Irregular migrants	Travelers coming for a short-term stay	Visa free travellers
Interoperability envisaged	<i>Yes, allows for future interoperability with other information systems according to Eurodac proposal (2016)</i>	No	<i>Yes, SIS II proposal on police cooperation (2016) states that it may be revised to reflect interoperability</i>	<i>Yes, SIS II proposals on border and return (2016) state that they may be revised to reflect interoperability</i>	<i>Yes, VIS-EES (verify visa holders)</i>	<i>Yes, ETIAS-EES (common hardware and software components) ETIAS-EES, VIS, Europol, SIS II, Eurodac, ECRIS (risk assessment)</i>

Note: Proposed systems and proposed changes in italics.

Source: FRA, based on existing and proposed legal instruments (as of April 2017)

and right to access international protection, as well as the fundamental rights implications that interoperability may have on the rights of migrants in an irregular situation or in the context of profiling.

1

Data protection: data minimisation, purpose limitation and data retention



According to Article 8 (1) of the Charter, everyone has the right to the protection of their personal data. Article 7 of the Charter stipulates the right to respect for private life. This section describes the implications on the protection of personal data when processing biometric data. It then notes how the principles of data minimisation, purpose limitation and storage limitation may be subject to new fundamental rights challenges when IT-systems become interoperable.

Under the current legislative framework, protection of personal data is regulated by Directive 95/46/EC³² and, when it concerns police and judicial cooperation in criminal matters, by Council Framework Decision 2008/977/JHA.³³ Both instruments contain provisions on the right to information, the right of data subjects to access information about themselves, the right to an effective remedy, obligations in the field of data security, the right to amend incorrect data, and rules on sharing data with third parties. In 2016, both instruments were replaced by a new legislative framework, Regulation (EU) 2016/679 (General Data Protection Regulation)³⁴ and Directive

(EU) 2016/680.³⁵ These new instruments reflect technological and other developments and overall offer a more comprehensive set of safeguards. Both new instruments must be fully incorporated into national law by May 2018. This paper looks at the data protection relevant implications of interoperability in the context of this new legislative framework.

Where the controller is an EU institution, agency or body, Regulation (EC) No. 45/2001³⁶ applies, until the European Commission proposal on the processing of data of EU institutions and agencies is adopted.³⁷

The instruments setting the legislative framework governing data protection also apply to EU large-scale information systems. The legislative acts of each of the individual systems contain specific provisions determining the controller, competent authorities whose staff can access the data, purposes of processing, storage periods and specific modalities related to, for example, sharing with third countries. As a result, the specific data protection rules and safeguards applicable to

³² 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, OJ L 281/31.

³³ 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, OJ L 350/60.

³⁴ 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 May 2016, p. 1-88.

³⁵ 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 May 2016.

³⁶ 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, OJ L 8/1.

³⁷ European Commission (2017), *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/EC*, COM(2017) 8 final, Brussels, 10 January 2017.

the data in each individual IT-system differ, and these differences need to be reflected also by the selected interoperability solution.

The right to protection of personal data is not an absolute right. Interferences with this right can be justified, but have to respect the requirements of the Charter and of the ECHR. Under EU law, any limitation on fundamental rights guaranteed by the Charter must be in line with the requirements of Article 52 (1) of the Charter, namely: limitations must be provided for by law, must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, respect the essence of the right, and be proportionate.³⁸ The aim of any such limitation, therefore, needs to be carefully considered. The CJEU has underlined that all the above requirements must be complied with and that an objective of general interest is not, in itself, sufficient to justify an interference.³⁹

Any option for interoperability affects the right to protection of personal data, with implications in relation to the data protection principles of purpose limitation, data minimisation and storage limitation. The interference is also higher if biometric data are processed. The concept of data protection by design and by default (commonly referred to as ‘privacy by design’)⁴⁰ is often highlighted as a precondition for establishing interoperability in line with core data protection principles.⁴¹ This concept aims to provide solutions that fully respect privacy and data protection principles without hampering the functionality of information systems. It applies at all stages of processing, and increases transparency to the data subjects.

1.1. Biometric data

Alphanumerical data can be unreliable for establishing the identity of a person, due to many so-called aliases, cases of identity fraud, entry and spelling mistakes. Therefore, they may lead to linking database entries to the wrong person. This may have significant negative consequences for the person concerned – for example, the arrest of the wrong person by the police. The

use of biometric data to search the different IT-systems renders the matching significantly more reliable. The power of biometric data lies in their capacity to serve as universal identifiers allowing information about the same person to be linked across different information sources.⁴²

IT-systems increasingly rely on biometrics, as Table 2 shows. EU systems rely primarily on fingerprints, with facial images increasingly used as a second biometric identifier. The age from which biometric data are collected is being reduced, with Eurodac amendments proposing processing of fingerprints and facial images of children as of six years of age.

Biometric data, however, represent a special category of personal data. Under Article 9 of the General Data Protection Regulation (GDPR), the processing of this data is generally prohibited. The prohibition does, however, not apply where processing is “necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.

The General Data Protection Regulation defines biometric data as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (Article 4 (14)). The definition of biometric data applies to photographs only when these are processed through specific technical means allowing the unique identification or authentication of a natural person (Recital 51).

The processing of facial images or fingerprints requires particular guarantees.⁴³ For biometric passports, the CJEU has indicated that central storage of biometrics would need to comply with more stringent requirements than their storage in the passport itself.⁴⁴ In *M.K. v. France*, the ECtHR concluded that retention of fingerprints solely for the reason of preventing future identity theft would, in practice, be tantamount to justifying the storage of information on the entire population, which is clearly excessive.⁴⁵ In its opinion on the proposed Entry-Exit System, the European Data Protection Supervisor (EDPS) underlined that any proposed system requiring

38 See also CJEU, C-73/07, *Satakunnan Markkinapörssi and Satamedia*, 16 December 2008, para 56; C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, 9 November 2010, para 77; Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014, para 52, and C-362/14, *Schrems*, 6 October 2015, para 92.

39 See for example CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014, para 51.

40 The principle of data protection by design and by default is reflected in the General Data Protection Regulation (Regulation (EU) 2016/679) (Recital 78 and Article 25), and in Directive (EU) 2016/680 (Recital 53 and Article 20).

41 EDPS (2010).

42 Mordini, E., Green, M. (2009), p. 11.

43 ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras: 68, 84 and 85; General Data Protection Regulation (Regulation (EU) 2016/679), Article 9(1); Directive EU 2016/680, Article 10.

44 CJEU, C-291/12, *Schwarz v. Bochum*, 17 October 2013, paras 59–63.

45 ECtHR, *M.K. v. France*, No. 76100/13, 18 April 2013, para 40.

Table 2: Biometric data in existing and planned IT-systems

	Eurodac	VIS	<i>SIS II: police</i>	<i>SIS II: immigration control</i>	<i>EES proposal</i>	<i>ETIAS proposal</i>
Biometrics included	Fingerprints as of the age of 14 years, and fingerprints and facial image as of the age of 6 years, according to Eurodac proposal (2016)	Fingerprints and facial image as of the age of 12 years	<i>Fingerprints, facial image, DNA profile (missing persons for protection reasons), according to SIS II proposal on police cooperation</i>	<i>Fingerprints and facial image, according to SIS II proposals on borders and return</i>	<i>Fingerprints and facial image as of the age of 12 years</i>	No

Note: Proposed systems and proposed changes in italics.

Source: FRA, based on existing and planned legislative instruments (as of April 2017)

the processing of biometric data should be accompanied by sufficient safeguards to ensure the effective protection of data stored against the risk of abuse, mistakes, unlawful access or use. Such safeguards would contribute to making the system more proportionate, as also stated by the EDPS.⁴⁶

1.2. Data minimisation

Article 5 of the General Data Protection Regulation spells out the principle of data minimisation, whereby personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. In this manner, the reference to ‘necessity’ under the General Data Protection Regulation goes beyond the wording of Directive 95/46/EC, which required under Article 6 (1) (c) that the data are ‘not excessive’ in relation to the purposes. Data minimisation refers to both the amount of data collected and the data processed.

The current trend in IT-systems is not only to process more biometric data, but also an increasing amount of alphanumeric data about an individual. More data are stored in individual systems, including sensitive data. This has an impact on interoperability. First, it will allow the viewer to see more data on a specific individual in one search, which would provide a more complete set of information on the individual. Second, it may allow the viewer to get to know if information on an individual is stored in another system, even if s/he cannot see the content of such information (so-called “flagged” hits) because of rules on authorised access. Third, in case of a common repository of data, it will allow to store “links” and possibly “flagged” hits.

46 EDPS (2016), para 38. In this context, see also FRA (2015b).

1.3. Purpose limitation

Purpose limitation is a central question when discussing interoperability. The principle of purpose limitation provides that personal data may be processed only for specified purposes that must be explicitly defined.⁴⁷ The principle is mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the General Data Protection Regulation. According to the regulation,⁴⁸ personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. The person concerned should be able to foresee the purpose for which his or her data will be processed.⁴⁹

Each of the EU databases has been established for a specific purpose, defined in the corresponding legal instruments. Table 3 provides an overview of the primary purpose of existing and planned information systems.

The architecture of each information system and the accompanying safeguards reflect its purpose. In essence, the current compartmentalised nature of the EU databases in itself acts as a safeguard against the use for unauthorised purposes. The European Commission emphasised this already in 2010, noting that an overarching EU information system would “constitute a gross and illegitimate restriction of individuals’ right to privacy and data protection and pose huge challenges in terms of development and operation”.⁵⁰ This reflects

47 See also Article 29 Data Protection Working Party (2013).

48 See also Directive 95/46/EC, Article 6 (1) (b), and Regulation (EC) No. 45/2001, Article 4 (1) (b).

49 CJEU, C- 275/06, *Promusicae v. Telefónica de España SAU*, opinion of Advocate General Kokott delivered on 18 July 2007, para 53.

50 European Commission (2010), *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, 20 July 2010, p. 3.

rulings of the ECtHR⁵¹ and the CJEU,⁵² which highlighted that decentralised storage of personal data mitigates the risk of abuse for other than permitted purposes.

In its ruling invalidating the Data Retention Directive, the CJEU pointed to the fact that the directive did not expressly provide that access and the subsequent use of the data must be strictly restricted to the purpose of combating precisely defined criminal offences, but relied instead on EU Member States to define the procedures. According to the court, the legislator failed to lay down objective criteria for limiting the number of persons authorised to access and use the data to what is strictly necessary to the objective pursued.⁵³

Purpose limitation has particular relevance in the context of law enforcement access to the individual IT-systems. For most of the existing systems (Eurodac and VIS), access for law enforcement to combat terrorism and other serious criminal offences was introduced at a later stage as an additional purpose.⁵⁴ As such, it is limited by purpose and in scope and subject to specific conditions. The need to retain the safeguards specific to each system and purpose should be at the core of any interoperable solutions.

In the context of interoperability, a challenging question is whether an officer should be made aware of the existence of information that is available on a person in

Table 3: Primary and additional purposes in existing and planned IT-systems

	Eurodac	VIS	SIS II: police	SIS II: immigration control	EES proposal	ETIAS proposal
Main purpose	Application of Dublin	Visa and border procedures	Alerts to help fight crime	Alerts on refusal of entry and stay <i>Return decisions included in SIS II according to SIS II proposal on return (2016)</i>	<i>Registration of entry and exit</i>	<i>Pre-border checks</i>
Added purpose: Apprehension and return	Yes	Yes	No	No	Yes	No
Added purpose: law enforcement (serious crimes and terrorism)	Yes	Yes	No	No	Yes	Yes

Note: Proposed systems and proposed changes in italics.

Source: FRA, based on existing and planned legislative instruments (as of April 2017)

51 ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, para 103.

52 CJEU, C-291/12, *Schwarz v. Bochum*, 17 October 2013, para. 55.

53 CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014, paras 61-62.

54 See 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, OJ L 218/129, and 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), OJ L 180/1.



one of the interoperable databases but that the officer is not authorised to access, in line with access rules as laid down in the respective legal instruments – so-called “flagged hits”. While it is clear that the officer does not have the authority to view the content of this information, the simple knowledge that more is stored on the individual in a particular IT-system may already give hints to the officer on that individual which he or she would otherwise not have. For example, the knowledge of an entry in Eurodac would give the officer a clue that the individual entered the EU in an unauthorised manner and/or applied for asylum. This may influence the officer’s conduct. In principle, providing the officer information about a hit he or she is not entitled to see would represent a ‘function creep’.

Europol has actually developed a mechanism for controlled access to its databases that addresses the situation that in some instances the searching officer should remain unaware of “flagged hits”. In case the Member State that owns the data has indicated that its data cannot be shared without prior consent, this Member State will first be notified concerning the hit by another Member State and will then decide whether or not to follow up on the hit.⁵⁵

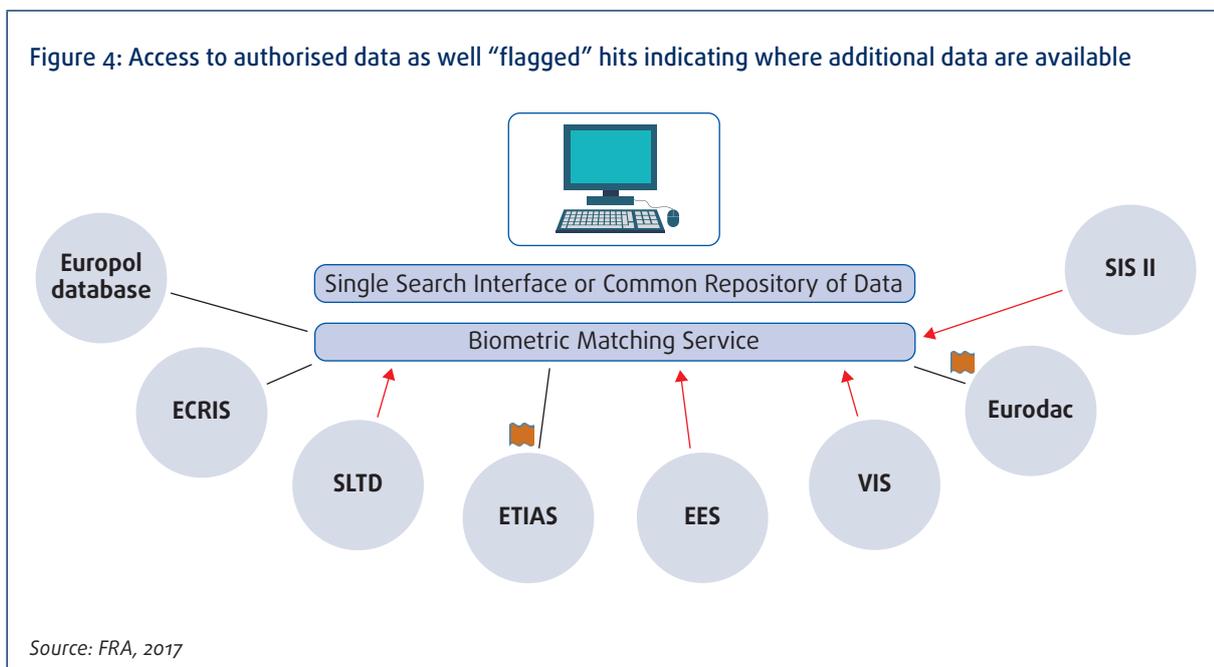
A single search interface or a common repository of data can make the officer aware of the existence of additional data about the person that he or she is not authorised to access under the respective legal

instruments, by showing “flagged” hits. In case such data are registered under another identity, the officer can also identify multiple identities in this way, which may be particularly important for security reasons. Figure 4 illustrates a situation where the officer is authorised to access SIS II, VIS, EES and SLTD, in line with the respective legal instruments. However, through the “flagged” hits, the officer also gets to know that data on the person in question are stored in Eurodac and ETIAS,⁵⁶ but he or she cannot access this data, in line with rules on authorised access as laid down in the respective legal instruments.

1.4. Storage limitation

Retention of personal data must not go beyond what is necessary for the purposes for which the personal data are processed (principle of storage limitation, Article 5 (1) (e) of the General Data Protection Regulation). The ECtHR has dealt with the length of retention in relation to biometric data. In *M.K. v. France*, the ECtHR held that the retention of fingerprints in a database for 25 years collected in relation to all criminal offences irrespective of their seriousness constituted a disproportionate interference with the applicant’s right to respect for his private life, and cannot be regarded as necessary in a democratic society. In *S. and Marper*, it underlined that a blanket and indefinite retention of biometric data of persons suspected but not convicted of offences fails

Figure 4: Access to authorised data as well “flagged” hits indicating where additional data are available



Source: FRA, 2017

55 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, L135/53, 24 May 2016, Article 20 (2).

56 On ETIAS and fundamental rights in general, see FRA (2017).

Table 4: Data retention periods in existing and planned EU IT-systems

	Eurodac	VIS	SIS II: police	SIS II: immigration control	EES proposal	ETIAS proposal
Data retention	Applicants for international protection, 18 months; <i>10 years, according to Eurodac proposal (2016) and apprehended persons: 5 years</i>	Visa applicants 5 years	Alerts for 3 years and then review the need to keep the alert; <i>5 years, max. according to SIS II proposal on police cooperation</i>	Alerts for 3 years and then review the need to keep the alert; <i>5 years, max., according to SIS II proposals on border and return</i>	<i>Short-term travellers 5 years</i>	<i>Visa free travellers 5 years</i>

Note: *Proposed systems and proposed changes in italics.*

Source: FRA, based on existing and planned legislative instruments (as of April 2017)

to strike a fair balance between the competing public and private interests.⁵⁷

Storage periods under the individual legal instruments of existing and planned EU IT-systems have been designed to reflect the varying relevance of the data over time, as illustrated in Table 4. Although the new proposals tend to align retention times, the logic of different retention periods reflecting the purpose of the individual IT-systems remains valid.

Conclusions

Interoperability solutions should be developed and designed taking into account the right to data protection, with due regard to the state of the art.

Any interoperable solution or solutions selected for the EU IT-systems will need to be designed in a manner that does not unduly affect core data protection principles. This includes respect for the limited purposes of each individual EU IT-system, its specific safeguards and storage (retention) periods, all of which reflect the nature of the data contained therein. Where the chosen solution leads to additional fundamental rights interference, such interference needs to pursue a clearly demonstrated legitimate aim and meet the conditions of Article 52 (1) of the Charter.

Interoperability needs to respect the special sensitivity of biometric data and take into account the need for specific safeguards when such data are processed. It should not lead to the collection and processing of more – biometric or alphanumeric – data than are necessary for the existing purposes under the individual legal instruments. Technical solutions chosen must limit access only for authorised purposes and to authorised staff. Such solutions must provide for automated deletion of data to comply with legally set retention times. The biometric matching service and the single search interface should not be programmed to actually store data but only to match it.

If interoperability solutions envisage the possibility to show “flagged” hits, which would inform the officer about the existence of additional data that he or she is not authorised to access according to present rules, adjustments may be necessary to the legal instruments establishing the different information systems. There would be a need to assess the necessity of adding an additional purpose to each instrument covered by interoperability and/or of drafting a specific new legal instrument on interoperability. The knowledge of existing additional information about a person, such as an entry in SIS II, possibly under another name, may support the identification of that person and influence the decision-making.

Alternatively, a mechanism for informing responsible authorities without the viewing officer becoming aware of the “flagged hit” could be envisaged, comparable to the mechanism that Europol has developed for allowing controlled access to its databases. Building on the Europol example, a mechanism could be considered that would not reveal “flagged hits” to the end user but to the relevant authority in his or her Member State, following an assessment of legal, practical and technical implications.

57 ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, para. 125. Some of the currently pending ECtHR applications may provide additional clarity on the compliance of the retention of biometric data with the right to private life, particularly *Djalo v. the United Kingdom*, No. 17770/10, *Hall v. the United Kingdom*, No. 21457/11, *Gare-Simmons v. the United Kingdom*, No. 71358/12 and *Murphy v. the United Kingdom*, No. 51594/10, all communicated on 10 December 2014.

2

Fundamental rights risks of unlawful access or use of personal data



Prevention of unauthorised access and use of personal data are key elements of data security. It is necessary to give full effect to the principle of purpose limitation and to prevent other fundamental rights violations. FRA research shows that instances of unauthorised access occur. For example, two court cases in Bulgaria⁵⁸ and the Netherlands⁵⁹ involved unauthorised access to SIS II and subsequent sharing of the information with third parties, which was in both cases punished with disciplinary measures. Awareness of the need to verify rigorously access rights may also be limited, leading to the risk of unauthorised access, as FRA research showed. Experts providing legal advice to asylum applicants who were interviewed noted, for example, in Germany: *“I only have to know the name and the date of birth of a given person, maybe the case number, and can get data which has been recorded in such systems from the police or other authorities, without power of attorney. I do it all the time. I do have power of attorney for that, but nobody asks for it.”*

Protection from unauthorised access to personal data is enshrined in both EU law (Articles 5 (1) (f), 28 and 32 of the General Data Protection Regulation) and in Article 7 of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108). It includes the duty of the data controller to have a record system that allows

tracking who has accessed the data and when.⁶⁰ It is closely linked to the duty to set clear rules on who can access the data collected.

In the *Digital Rights Ireland* case, the CJEU has clarified that EU legislation providing for the collection and retention of personal data must impose sufficient guarantees to protect effectively personal data against the risk of abuse and against any unlawful access and use of that data.⁶¹ The quantity and sensitive nature of the data needs to be taken into account. The need for such safeguards is all the greater where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.⁶² The CJEU highlighted in relation to the issue of unlawful access to the data, the need to have in place rules that would “serve to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality”.⁶³ Legislation regulating access to retained data must lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data. In its recent *Tele2* ruling, the court underlined that national legislation must be based on objective criteria defining the circumstances and conditions under which the competent national authorities are to be granted access to the data.⁶⁴

Personal data that are unlawfully accessed or shared may have serious implications for other fundamental

58 Bulgaria, Regional Directorate of Internal Affairs district 4, Ordinance No. 3 from 22 August 2013, issued by the head of Sofia (Заповед, рег. № з - 318 от 22.08.2013 г., издадена от началника на 04 РУП при Столична дирекция на вътрешните работи), the appeal was rejected by the Administrative Court – Sofia (Административен съд – София), Decision No 7660 of 5.12.2013 on administrative case No 9526/2013 (Решение № 7660 от 5.12.2013 по адм. д. № 9526/2013).

59 Netherlands, District Court Alkmaar (*Rechtbank Alkmaar*) (2011), Case No. AWB 10/2526, 15 December 2011.

60 See for example ECtHR, *I. v. Finland*, No. 20511/03, 17 July 2008.

61 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014, para. 54 with further references.

62 *Ibid*, para. 54 and 55.

63 *Ibid*, para. 66.

64 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Secretary of State for the Home Department*, 21 December 2016, para. 119.

rights, beyond data protection. Interoperable databases are likely to become more attractive for those trying to access personal data by illegal means, such as organised crime groups or even hackers linked to foreign states. Large amounts of personal data are highly attractive for a range of criminal activities as well as state sponsored hacking by hostile regimes. The risk of information leaks is particularly high for persons in need of international protection (see [Section 5](#)).

The risk of unauthorised access to and use of personal data increases with broader accessibility of information stored in the various databases, which is the underlying rationale of interoperability. Four aspects are examined in this section:

- indirect access;
- access by private persons;
- increased number of access points;
- sharing with third countries.

2.1. Indirect access

A staff member can have direct access to the data through the IT-system or indirect access by requesting another officer or branch to carry out a search. According to FRA research carried out in 2015, indirect requests for accessing Eurodac, for example, are the exception in the EU, but they are still allowed in some EU Member States.

In these cases, the officer who is requested to access the data on behalf of another officer has to examine whether or not to share the personal data collected. He or she has to verify if the officer requesting the information is entitled to receive it and, if so, to which information he or she has access and to which not.

Errors in such a validation procedure, which could lead to unauthorised access to information, would have more severe consequences in a situation of interoperability, as more data would be available in one search.

2.2. Access by private persons

Two planned IT-systems – the proposed ETIAS (Articles 14 and 39) and the proposed EES (Article 12) – will allow access by private persons and carriers, such as flight companies, to a specific and very limited subset of data (namely for requesting a travel authorisation or checking its status of the travel authorisation in the context of ETIAS and checking the status of the visa in the context of EES).

Where these entities are only supposed to have access to a particular segment of the data, this segment needs to be precisely defined and isolated from the rest of the database in a manner that ensures that other data or data of other persons cannot be accessed. As pointed out by the EDPS, any access to the system should be limited only to authorised staff working for the private entity (carrier). Moreover, such access should be based on a proper authentication scheme, it should be logged and safeguards should also extend to the processing of data after their extraction by the third party.⁶⁵

Since ETIAS and EES envisage access through an internet interface, particular safeguards to uphold access rights would need to be in place. This is particularly important because a data security breach in case of interoperable systems could lead to unauthorised access to large amounts of data.

2.3. Increased number of access points

Ensuring data security of interoperable systems may become more difficult as the number of points of entry used to access the system increase. If databases can be accessed from terminals located in third countries or in locations that host third-country liaison officers, they could become more accessible to unauthorised persons.

This risk is further exacerbated if interoperable systems are accessed through mobile devices. While facilitating access for the authorised personnel, mobile solutions increase the risk of both unauthorised access by obtaining physical access to the devices or hacking less secure connections. Unauthorised sharing of data poses a risk as well – for example, where an officer uses his or her access rights to search for the data of a specific person and transmits them to third parties, typically for personal gain. The use of the internet for providing access would also require particular safeguards to ensure that access rights are upheld.

In its opinion on the Entry-Exit proposal, the EDPS highlighted that the security of a system that is spread across multiple entities requires a holistic approach. This means not limiting oneself only to the security of the central units and the communication channels between the interconnected databases (in this case EES and VIS) but addressing all parts and users of the system, including the secure connection to the national border infrastructure of each Member State (e.g. responsible offices at individual border crossing points). Weakened security of any part of the interconnected system would affect

⁶⁵ EDPS (2016), paras 48-53.



the security of the system overall.⁶⁶ This is even more so the case where IT-systems are interoperable.

2.4. Sharing with third countries

The new EU data protection framework (see Article 46 of the General Data Protection Regulation) as well as the individual legal instruments establishing the various EU databases regulate the transmitting of data to third countries. However, due to the different types of data stored in the individual IT-systems, data sharing with third countries and international organisations is regulated differently in each of the existing or proposed information systems, as illustrated in Table 5. For example, the proposed ETIAS Regulation (Article 55) contains an explicit prohibition for EU Member States to share the information contained therein with third countries, international organisations and private entities (with the exception of Interpol). In contrast, the proposed EES Regulation (Article 38 (2)), the SIS II proposal on return (Article 10), the VIS Regulation (Article 31) and the proposal for a revision of the Eurodac Regulation (Article 38) allow for sharing personal data with third countries to identify a third-country national for the purpose of return, albeit with some exceptions. To facilitate police cooperation, a Member State may

also under certain conditions share SIS II data through Europol (Article 41), Eurojust (Article 42) and Interpol (Article 55), according to Council Decision 2007/533/JHA.

Interoperability will make access to data easier and therefore increase the risks that data are unlawfully shared with third countries.

Sharing personal data with third countries can lead to particular risks in case of asylum applicants, where they or their families may be subject to retaliation measures ranging from criminal sanctions upon return to persecution of family members. In general terms, there is a prohibition to share information that a person applied for international protection in the EU with third countries,⁶⁷ although safeguards are not always systematically followed, as FRA research showed. Typically, information is shared to obtain the assistance of the country of origin for purposes of identifying the third country national. Civil society organisations reported, for example, that Bulgaria shared all fingerprints of asylum seekers claiming to be Syrians with the Consular Section of the Syrian Embassy and that this has put the safety of the concerned persons at risk.⁶⁸ Lawyers interviewed in FRA research also mentioned Polish cases when the status of Vietnamese persons as asylum seekers were not correctly registered in the IT-systems and they were

Table 5: Purposes allowing sharing data with third countries in existing and planned EU IT-systems

	Eurodac I	VIS	SIS II: police	SIS II: immigration control	EES proposal	ETIAS proposal
Data sharing with third countries	<i>For return purposes, according to Eurodac proposal 2016</i>	For return purposes	Only by Europol and Eurojust with the consent of the Member State who issued the alert, and by Interpol for checking against Interpol databases (SLTD)	<i>For return purposes, according to SIS II proposal on return (2016); only by Europol with the consent of the Member State who issued the alert, according to SIS II proposal on border checks (2016)</i>	<i>For return</i>	<i>No, only for checking against Interpol databases (SLTD and TDAWN)</i>

Note: Proposed systems and proposed changes in italics.

Source: FRA, based on existing and planned legislative instruments (as of April 2017)

⁶⁷ This is expressed in Article 48 of the Asylum Procedures Directive (Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348), as well as in Article 35 of the present Eurodac Regulation.

⁶⁸ European Council of Refugees and Exiles (2013).

⁶⁶ Ibid, paras 42 and 43.

treated as irregular migrants subject to return and not in need of protection.

The ECtHR also noted that communication between the authorities of the host country and the consular services of the country of origin for the purpose of return, without explicitly informing that the person has applied for international protection, may give the country of origin sufficient information from which it can be inferred that the person is a rejected asylum seeker.⁶⁹

To mitigate the risk of serious harm for asylum applicants or their families, the proposed changes to the Eurodac Regulation clearly forbid the sharing of information that the individual applied for asylum (Article 38). The existing safeguard which bans the transfer of personal data to third countries if there is a real risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights, also continues to apply. The scope of this safeguard is however limited to data which are exchanged between Member States following a match in Eurodac. In its 2016 legal opinion on the proposed Regulation, FRA suggested that this safeguard should also apply to personal data stored in the system and not only to data exchanged after obtaining a match.⁷⁰ Given the steady increase in data collected in individual databases, interoperability can further exacerbate the risk that the data communicated to third countries may be sufficient to identify a person as an asylum seeker or give indications – for example, based on the length of stay – of conduct. This may lead some countries of origin to threaten or harm the person or his or her family members.

Sharing of data often occurs in the framework of EU or bilateral readmission, or law enforcement agreements. Data could then be shared with third countries along principles similar to those used in the Prüm cooperation, namely through comparison against each other's biometric databases on a hit/no-hit basis. This provides the possibility for a very precise identification of an individual in the third country, which may, in certain situations, expose the person and his or her family members to serious harm.

Conclusions

One of the pillars of any interoperable solution must be strong data security measures to prevent unauthorised access and sharing of personal data. Points of entry to the systems, particularly mobile devices, would need to be secured against unauthorised access. With more data becoming accessible to more people, the risk of unlawful use increases.

In some EU Member States or for some IT-systems, staff members who do not have direct access to the data stored may request a colleague to access the system, indirectly providing them access to data. Therefore, enhanced verification measures are needed to prevent abuse. Where officers request indirect access to information stored, effective verification procedures are necessary to determine if the requesting person is authorised to receive the information and, if so, to what extent.

If interoperability is implemented through a single search interface that becomes the default search tool (replacing the IT-specific search tools), segments of databases accessible to private persons would need to be completely isolated from the rest of the IT-systems.

To limit the risk of both unauthorised access, as well as sharing with third parties, in an interoperability situation where there are a significant number of logs, logging of all uses should not only occur on the basis of the user profile but also by purpose. Interoperability solutions would need to ensure that safeguards such as the prohibition of exchange of personal data with third countries would apply horizontally. In particular, they would need to do this regardless of whether the data have been in the first place obtained directly from the system or, for example, through a single search interface or a common repository. In this manner, the data would need to remain 'linked' to the source and sharing would remain subject to the original safeguards applicable to the source database.

69 ECtHR, *F.N. and Others v. Sweden*, No. 28774/09, 18 December 2012, paras 74-76.

70 FRA (2016b), p. 31.



3

Fundamental rights consequences of taking decisions on the basis of low quality or unlawfully stored data



This section examines the impact of low quality and unlawfully stored data on an individual in an interoperable setting. It first looks at alphanumeric data and then at biometric data. This section then discusses in greater detail the right to access one's own personal data and the right to have it rectified, together with the right to rebut a false assumption based on the data stored.

Under the principle of data accuracy, reflected in Article 5 (1) (d) of the General Data Protection Regulation, as well as Article 4 (1) (d) of Directive (EU) 2016/680, the controller should not use information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. The controller should take "every reasonable step [...] to ensure that personal data that are inaccurate [...] are erased or rectified without delay".⁷¹ For instance, the Council Working Party on Information Exchange and Data Protection (DAPIX) addresses data quality.⁷² The EDPS has also underlined the importance of data accuracy in light of the risk of severe negative consequences for the person concerned.⁷³ The interim report of the High Level Expert Group on information systems and interoperability has also highlighted this.⁷⁴

The obligation of the controller to keep data accurate and up to date is not limited to situations where the data subject requests a rectification. For example, before a foreigner who is subject to an entry ban can be issued a residence permit, the EU-wide applicability of the entry ban needs to be removed. To do so, the EU Member State that intends to issue the residence permit will have to inform the Member State who issued the

entry ban, in accordance with Article 25 of the Schengen Implementing Convention and Article 11 (4) of the Return Directive.

Data entered in an information system could be based on a flawed administrative decision. For example, a decision to issue an entry ban (which is subsequently recorded in SIS II) must be balanced against the right of the foreigner to enjoy his or her family life. Past interventions by the Greek Ombudsman illustrate that such assessment of proportionality does not always take place affecting the data subject's right to respect for family life.⁷⁵ An entry ban record in SIS II would in many instances lead to an automatic rejection of a visa application.

Inaccurate or unlawfully stored data can concern both alphanumeric and biometric data. Interoperability may multiply the effects of inaccurate data since it offers results from databases that otherwise would not necessarily be consulted. It may, however, also make it possible for the authorities to spot inconsistencies and errors, and initiate measures to rectify them. Interoperability intends to improve the decision-making process by offering access to comprehensive data in a simple form. If the information received is not reliable – meaning that it is inaccurate and/or unlawfully stored (for instance, not deleted when it should have been) – the quality of decisions taken will be affected.

On the other hand, in case a person disputes some of the information, other data stored may support the claim of this person. Making more data available about a person may support the lawfulness of the decision-making.

71 General Data Protection Regulation (Regulation (EU) 2016/679), Article 5 (1) (d).

72 Council of the European Union (2016a).

73 EDPS (2008), p. 2.

74 High Level Expert group on Information Systems and Interoperability, *Register of Commission Expert Groups*.

75 Greek Ombudsperson, Human Rights Section, *Intervention case no 1709/08/5*, 29 November 2010, decision available in Greek; Greek Ombudsperson, Human Rights Section, *Intervention case no 15767/451312012*, 20 December 2012.

3.1. Alphanumeric data

Many factors affect the reliability of the alphanumeric data in a system. According to the findings of the FRA project on biometrics, these include: spelling errors; lack of documents provided by a person; insufficient language skills by the officer; technical deficiencies; incorrect transcription of names into the Latin alphabet; cultural norms determining the usage of first and second names; recording of birth dates when the precise date is unknown; lack of skills and training; or situations where the common format for data transmissions is not followed. Increased workload and strain on the staff recording and dealing with data may also contribute to the frequency of mistakes. This was particularly evident following the large arrivals in the autumn of 2015.

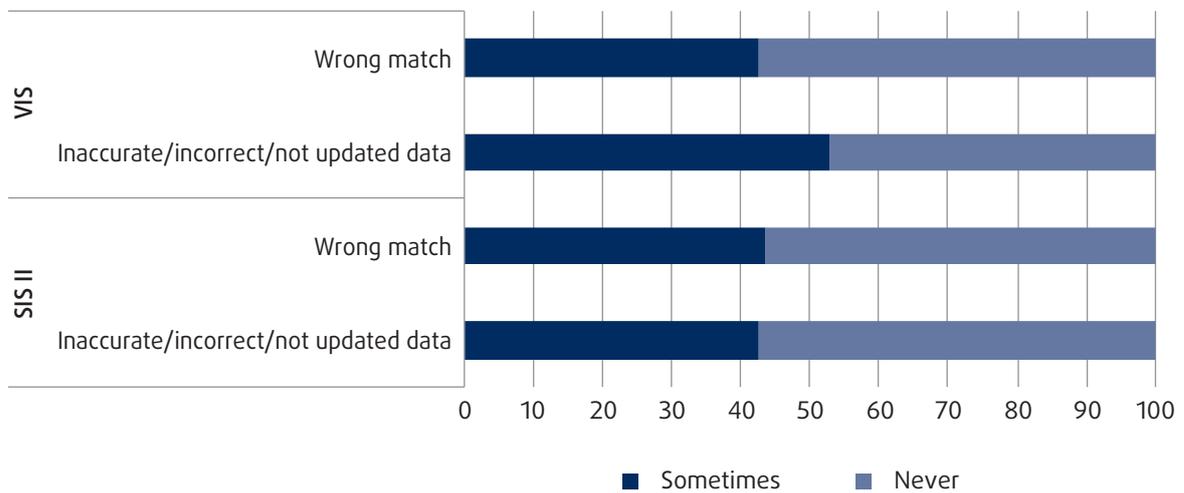
The EU IT-system relies on data included in a national database, which can create both risks and opportunities. If the data are inaccurate, the mistake is multiplied. But if the system relies on national databases having a good quality management process, as is the case in some EU Member States in relation to SIS II, the risk of mistakes is mitigated. In practice, as pointed out by a Belgian public official, often a mistake is only identified

when data are checked against another database. Some public officials who FRA interviewed for the biometrics project have therefore expressed the opinion that technical solutions, such as interoperability between systems, may contribute to correcting systematically mistakes and inaccuracies.

The risk of mistakes is reduced if the person is actively involved in approving the data inserted, or he or she is provided the possibility to clarify contradictions when mistakes are discovered, according to public officials FRA interviewed for the project on biometrics. They stressed that double-checks, training and use of electronic readers to minimise manual entries, as well as automatic verification against other data entries, when applicable, could contribute to reducing the risk of mistakes.

In the small-scale survey that FRA carried out within the project on biometrics at Diplomatic Missions or Consulate Posts (DMCPs), staff were asked how often they or their colleagues experience that some of the personal data – such as name, sex, nationality or age – inserted in VIS or SIS II are inaccurate, incorrect or not updated. For SIS II more than 40 % of the staff and for VIS slightly more than 50 % indicated that incidents of

Figure 5: Experiences with wrong matches and inaccurate data in VIS and SIS II at DMCPs (%)



Note: The number of respondents varies for the replies, ranging from 39 to 53 persons. This is related to the fact that numbers of staff working with the databases at the actual DMCPs vary. The results are based on the following two survey questions:
 “Have you or one of your colleagues ever experienced that some of the personal data – such as name, sex, nationality or age – inserted in VIS or SIS II was inaccurate/incorrect/not updated?”
 “Have you or one of your colleagues ever experienced that some of the personal data - such as name, sex, nationality or age - inserted in VIS or SIS II matched with the wrong identity?”

Source: FRA project ‘Biometric data in large EU IT-systems in the areas of borders, visa and asylum’ – Biometrics DMCP staff survey 2016

wrong matches or inaccurate data sometimes occur in these databases (Figure 5).⁷⁶

Border guards participating in the small-scale survey also said that it frequently happened to them or their colleagues that persons who should be included in VIS because of having applied for a visa in the past could not be found in this IT-system. More than 60 % of respondents indicated that this happened at least once in the preceding 12 months. More than a quarter of respondents experienced this more than 10 times in the preceding year and some of them experienced this over 100 times. More than half of the border guards surveyed indicate that they at least sometimes experienced inaccurate, incorrect or not updated personal data – such as name, sex, nationality or age – in VIS or SIS II. Eurodac includes only very limited alphanumerical data: the EU Member State where the data was collected, gender, reference number, ID of authority, and dates (Article 11). While fewer respondents provided information on such experiences with Eurodac, still almost half of those providing information experienced such inaccuracies at least in some instances (Figure 6).

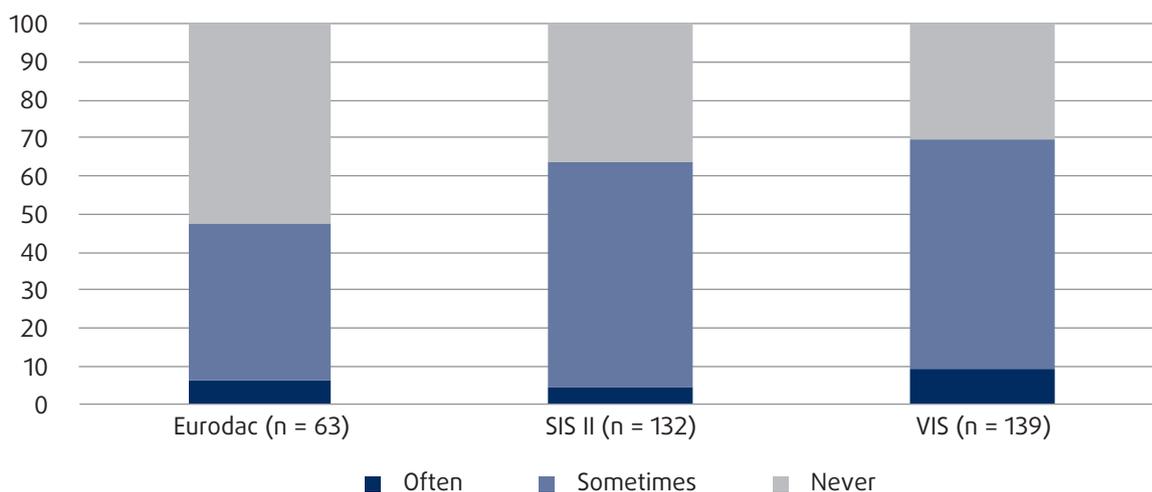
3.2. Biometric data

Biometric data are considered a reliable tool to verify the identity of a person. Nevertheless, although technology is evolving fast, the capturing and matching involve some risks of false matches, either “false accepts” or “false rejects”. Moreover, the reliability of the biometric identifier is of paramount importance for the officer to get to all data he or she is authorised to access, and in addition to detect persons with multiple identities, by identifying “flagged” hits. This section describes the two more commonly used biometric identifiers, namely fingerprints and facial images.

Fingerprints

A false biometric match due to poor fingerprinting quality can lead to situations where data on another individual are linked to the person. The quality of capturing or matching fingerprints can be influenced by many factors, such as age, manual work, humidity, dry, wet and untidy fingertips, unintentional as well as deliberate injuries to the fingertips, lack of training and technical difficulties. Captured and matched fingerprints have to meet set quality standards, defined and monitored by eu-LISA, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Figure 6: Experiences with inaccurate, incorrect or not updated personal data in Eurodac, SIS II and VIS



Note: The results are based on the survey question: “Have you or one of your colleagues ever experienced that some of the personal data – such as name, sex, nationality or age – inserted in VIS, SIS II or Eurodac was inaccurate/incorrect/not updated?”

Source: FRA project ‘Biometric data in large EU IT-systems in the areas of borders, visa and asylum’ – Border crossing points (BCP) survey 2016

76 FRA project ‘Biometric data in large EU IT-systems in the areas of borders, visa and asylum’ – Biometrics DMCP staff survey 2016.

Public officers interviewed by FRA in the project on biometrics expressed high trust in fingerprint matches, although some also concluded that they cannot know if it is a false match as the systems are never flawless. It often happens that the person claims that he or she has never been in the other Member State or has never applied for a visa to that Member State – both are relevant when determining which Member States will be responsible for assessing a claim for international protection. A lawyer interviewed in Sweden recalled several cases when asylum seekers ended up being transferred as Dublin cases: *“I don’t know how many. But, these are people who said in a very sincere way, I HAVEN’T been there”*. The lawyer concluded that it is in principle impossible to challenge a biometric match made by the authorities. Furthermore, the *Kamara* case illustrates how a false match can negatively affect individuals: the complainant was detained longer than lawfully permitted due to a false fingerprint match with another person.⁷⁷

The small-scale survey that FRA carried out within its biometrics project shows that every second border guard indicated that it had happened that the fingerprints did not find a match with those stored in VIS, although the person’s fingerprints should already be included in the system.

According to public servants interviewed as part of FRA’s project on biometrics, a more frequent problem is that the data profile of another person has been attached to the fingerprints, both in relation to Eurodac and VIS. Such a wrong link can result from administrative mistakes. The Eurodac ID number of another person may, by mistake, be connected to the fingerprints or the visa application of another person to the fingerprints. Consular staff of Belgium interviewed within the FRA biometrics project described the following situation: *“The staff were doing two applications at the same time and there is only one biometrics [reader/booth], and so they switched around (attached the biometrics to the wrong application). It happened in our embassy... so I imagine in small embassies in the world it can happen that people maybe are not well trained or they have so many applications that things get messed around.”*

Within one and the same IT-system a person can be registered under several categories. For instance, Eurodac can record a person as an asylum applicant, a recognised refugee, apprehended at the external border, or apprehended inside an EU Member State.

Facial image

Several factors may affect the quality of face images. The quality is affected by the interaction with the users (physical and behavioural), physical environment and equipment and processing systems. Other factors include outdoor operation, background and object occlusion, temperature and humidity, illumination and light reflection, ergonomics, time elapsed since the acquisition of the image, age, gender, ethnic origin and skin conditions.⁷⁸ All of them should be controlled so that face image quality is adapted to ICAO requirements.⁷⁹

When eu-LISA piloted facial image recognition in 2015, in more than 90 % of the cases a successful capture could be performed.⁸⁰ Facial recognition techniques have improved during the last years, but cases of lookalikes and twins may still lead to wrong matches. Furthermore, the time that passes between taking the picture and comparing it affects a correct matching. Changes in the facial shape of a child also have an impact on the reliability of a match – for example, when the image of a six year old child is compared five years later.⁸¹

Facial images captured by surveillance cameras could in principle also be used for matching purposes. This raises additional questions as the quality of the pictures often cannot be guaranteed. In addition, the use of surveillance cameras for purposes of asylum, border and visa management raises concerns in relation to issues such as the right to information and the principle of transparency as well as the right to privacy and protection of personal data in the broader sense.

3.3 The right to rebut a false assumption

Under Article 18 of the General Data Protection Regulation, the person can demand that the processing of the disputed data is restricted for a period enabling the controller to verify the accuracy of the personal data. This means that the controller must refrain from using the data pending the verification, including further sharing of the data, in order to ensure that possible false assumption can be rebutted before a decision is made. This is particularly important where the continued use of inaccurate or illegitimately held data could harm the person⁸² – for example, by denying entry or imposing detention. Although a derogation from this restriction is possible – for example, for reasons of important public

77 England and Wales High Court (Administrative Court), *Kamara v Secretary of State for the Home Department*, [2013] EWHC 959 (Admin), 26 April 2013.

78 Sanchez del Rio, J., Conde, C. et al., (2015).

79 International Organization for Standardization (2011).

80 eu-LISA (2015).

81 Aashmi, Sakshi Sahni, Sakshi Saxena (2014); Ramanathan, N., Chellappa, R., Biswas, S. (2009).

82 FRA and Council of Europe (2014), pp. 111-112.

interest – the use of such derogation would need to be assessed in line with the principle of proportionality and strike a fair balance between the rights at stake.

There is high trust in information provided in an IT-system, according to public officials, lawyers and experts interviewed by FRA. The reliability of a biometric match has also been upheld by national courts. For instance, in the United Kingdom, three asylum seekers disputed the Dublin transfer saying that they had not had an opportunity to contest the fingerprint evidence. The England and Wales High Court (Administrative Court) stated that a Eurodac match normally discharges the burden of proof on the Secretary of State and does not need to be corroborated. This puts the onus on the asylum seeker to produce evidence to disprove the match.⁸³

This was also the view of a Swedish lawyer who described the situation as follows: “It’s interesting that fingerprints are said to never be wrong, but it is obvious that there could be a wrong comparison, which could result in really severe consequences for the person concerned. And [there are only] small chances for us to prove that we are right, to show that the comparison is false. We are in the hands of the authorities who have the means to control these kinds of things. And it is difficult for us to access the documentation and get our point heard, because we have no one to ask for advice about the technical things.” In case of inaccurate alphanumeric data, at least some obvious mistakes, such as a misspelt name, can be rebutted by showing for instance personal data in documents and comparing additional data. This is generally not possible for biometric identifiers.

As highlighted above, interoperability could potentially magnify the effects of the decision-making on the individual caused by low data quality. When challenging the correctness of data, the data subject faces the burden of proof. A police officer interviewed in Germany for FRA’s biometrics project stated that there is a tendency among the staff of the competent authorities to assume that inaccuracies and mismatches are the result of right holders providing false information at some point. Partly for this reason, authorities tend not to take much into account the information provided by the migrant, unless they can verify it through entries in IT-systems or document evidence.

3.4 Right to access own data and have incorrect data rectified

The person whose data are being processed has the right to request access to his or her data from the controller. The right of access is recognised as a fundamental right in Article 8 (2) of the Charter, and is also included in Article 15 of the General Data Protection Regulation, as well as in Article 8 of the Council of Europe Convention No. 108, and in the legislative acts of the individual IT-systems. If inaccuracies are detected, the person has the right to the rectification of the data without undue delay (Article 16 of the General Data Protection Regulation and Article 16 of Directive (EU) 2016/680). Under Article 15 of Directive (EU) 2016/680, the right of access can be restricted, subject to the principle of proportionality, for specifically listed reasons, such as combating crime or protecting public security.

Ensuring the right of access to one’s own data, and to have it corrected where it is inaccurate, poses both legal and practical challenges in an interoperable system.

Given the circumstances in which the IT-systems are consulted, the person concerned would need to receive clear and unambiguous information on where and how to seek correction. In *Huber*, the CJEU clarified that the concept of necessity of data processing cannot have a meaning that varies among Member States, and that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data must be equivalent in all Member States.⁸⁴ The person would have to understand which IT-system is consulted, the purpose of the data processing, and who the controller is – thus the Member States’ duty to inform a central precondition.

Under Articles 13 and 14 of the General Data Protection Regulation, data subjects have the right to a comprehensive set of information, including information relating to the controller, the purposes of processing, any further recipients of the data, retention periods, as well as their rights as data subjects. In *Rijkboer*, the CJEU clarified that the active provision of information by the controller at the moment of collection does not reduce the obligation to give a data subject access to the information when the right of access is invoked.⁸⁵ Similar obligations exist under Article 13 of Directive (EU) 2016/680, although the controllers may restrict or delay the provision of information for specifically listed reasons, such as combating crime or protecting public

83 England and Wales High Court (Administrative Court), *R (on the application of YZ, MY and YM) v. Secretary of State for the Home Department*, [2011] EWHC 205 (Admin), 10 February 2011.

84 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008, para 52.

85 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkboer*, 7 May 2009, para 69.

security. The right to information is also reflected in the specific instruments discussed in this paper.

In a situation of interoperability the duty to inform would also extend to informing the person that if an officer accesses one specific IT-system he or she would also get to know that information is included in other IT-systems linked through interoperability. Data protection obligations in respect to data contained in different IT-systems but pertaining to the same person may belong to different bodies and be governed by different legislative frameworks – for instance, different legal instruments and controllers for Eurodac and SIS II. This would further blur responsibilities touching also on the right to an effective remedy.⁸⁶ For instance, the system would need to ensure that corrections made in one database are also visible when other databases are consulted, meaning that in case of a common data repository the maintained “views” are synchronised and updated.

Some categories of data may require special attention in relation to the right to rectification. This may, for example, be the case of data pertaining to children, given the limited legal capacity of children as well as the specific risks linked to the reliability of their data contained in the IT-systems, as outlined in [Section 4](#).

Conclusions

The quality of information stored in the different IT-systems is crucial for good decision-making. Currently, IT-systems store considerable amounts of inaccurate information and challenges are likely to persist, also when entering data in future. This could, for example, be an issue in situations where a large number of persons are processed and the administrations are under pressure.

Interoperability offers both opportunities and risks in relation to the quality and reliability of alphanumeric data. The risk of mistakes is reduced if correct information already included in one IT-system is taken over by another EU IT-system. If, however, the personal data that are re-used are incorrect, interoperability may lead to a multiplication of mistakes. Through interoperability, the authorities have more possibilities to become aware of inaccuracies. Authorities should therefore develop standardised procedures for automatic verification of data stored in other IT-systems and correct inaccurate data ex officio. This should be done by involving the person concerned when feasible, as authorities have a duty to erase or rectify without delay any inaccurate data.

In a situation of interoperability, the quality of the biometric identifier is of paramount importance. The

biometric identifiers considered in the discussions about interoperability are fingerprints as well as facial images, which are less accurate when used for searches. When searches are conducted using a facial image alone, the identity should be verified systematically against other biometric data or alphanumeric data before using the results of a match.

Due to the high degree of credibility attached to biometric data, as well as the technical complexity of its processing, it is difficult to rebut wrong assumptions based on biometrics. Interoperability would complicate this further, hence requiring additional safeguards to guarantee the rights of the data subjects. To give effect to the right to rebut a false assumption based on biometric data, the authorities would need to be open to address plausible arguments presented by the data subject.

In case a person would like to exercise the right of access to his or her own stored data, the person requesting such access and possibly rectification should not face an overly complicated procedure. Already at present, complex rules manage the processing of personal data in EU IT-systems, involving both national and EU bodies whose responsibilities are governed by different legal frameworks. The distribution of responsibility between the controllers and data processors of the common repository and those of the individual IT-systems would need to be clearly defined. This would involve taking into account the need to ensure that the complexities of joint control do not result in an unworkable distribution of responsibilities, which would hamper the effectiveness of data protection law.

Complying with the duty to inform may be additionally complicated in a situation of interoperability. The officer accessing the databases would first need to be clearly aware which database he or she is consulting, which may not be obvious when consulting several IT-systems, for example, through a single-search interface. Second, the officer would also need to know what his or her duties to inform the data subject are, as laid down in the legal instruments of the IT-systems in question. Not ensuring the right to information may make it impossible for the person concerned to exercise his or her right to access own data and have it rectified where necessary.

The correction of data already presents a challenge for the existing systems, particularly where the national authorities face an increased number of requests. Interoperability should be complemented by an increase in capacity to process these requests, to prevent the use of incorrect information as a basis for decisions that have a serious impact on fundamental rights. The system would need to take duly into account the limited legal capacity of children, and the ensuing need to involve parents or legal guardians in safeguarding the rights of children included in the databases.

⁸⁶ Article 29 Data Protection Working Party (2010), p. 18.



4

Rights of the child



Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions taken in relation to children by public authorities and private actors. Member States must provide to the child such protection and care as is necessary for the child's well-being and development. The best interests of the child is one of the four core principles of the UN Convention on the Rights of the Child. It is also reflected in the legal instruments establishing the individual EU IT-systems. Article 9 (2) of the proposed EES regulation, for example, stipulates that the best interests of the child shall be a primary consideration when retaining a child's data. Besides respecting Article 24 of the Charter, processing of children's personal data needs to comply with Article 7 (respect for private and family life) as well as Article 8 (protection of personal data).

The EU data protection *acquis* provides special protection to children with regard to their personal data,⁸⁷ and ECtHR jurisprudence expresses similar principles. In the case of *S. and Marper*, the ECtHR emphasised that blanket retention of biometric data by law enforcement authorities of persons not convicted of a crime may be especially harmful for children, given their special situation and the importance of their development and integration in society.⁸⁸ These arguments are also applicable where law enforcement or other authorities access data of children collected originally for other purposes. Asylum-seeking children whose data are collected in Eurodac are seen as a particularly vulnerable category. Retaining children's personal data, particularly biometric data, in migration-related databases can be particularly sensitive because such retention can greatly

affect their lives even though they had no say in their parents' decision to migrate.

The inclusion of more information on children is part of the current trend of making the EU databases more comprehensive. This includes the collection of biometric data which goes hand in hand with the inclusion of additional categories of alphanumeric data of the data subjects, such as the planned change of the Eurodac Regulation to also process the name, surname, nationality, date and place of birth and travel document information.

If the systems storing information on children become interoperable, the potential accessibility of the data expands. Given the particular vulnerability of children, it is essential that the principle of purpose limitation is strictly adhered to, and that individual officers are not made aware of the existence of any data that they are not authorised to access, which may be particularly challenging in case of a common repository of data. At the same time, interoperability offers new opportunities for child protection, provided child protection objectives are made more visible in existing systems.

4.1. Amplified effects of interoperability on children

For children, interoperability amplifies certain challenges common to all persons included in information systems. Two specific challenges are analysed here: the reliability of data and the risks of sharing criminal records.

87 See the General Data Protection Regulation, particularly Recital 38 and 58.

88 ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 124-125.

Reliability of children's data

The reliability of comparisons based on biometric data taken in the past may be lower, due to the ongoing physical development of the child. At present, fingerprints are collected in Eurodac for all children older than 14 years, and in VIS for those older than 12 years. Collection of fingerprints as of the age of 12 is included also in the proposed EES Regulation for third-country nationals entering the EU who are exempt from the visa obligation. The proposed recast Eurodac Regulation foresees reducing the age for the collection of fingerprints to six years.

According to scientific research, fingerprint recognition of children aged six years or above is under appropriate conditions achievable with a satisfactory level of accuracy.⁸⁹ FRA noted that whereas reliable matches can be made up to five years after the fingerprints have been taken, research does not allow drawing conclusions on the reliability of a match when more than five years have passed.⁹⁰ Given that the fingerprints of children applying for international protection may remain in the database for up to ten years, the margin of error when comparing children's fingerprints may be higher than for adults. False matches would affect both the functioning of the system as well as potentially disproportionately children's rights. A similar concern relates to the planned future introduction of facial image comparisons for Eurodac and the Entry-Exit System.⁹¹ False matches can affect a wide array of rights, including, for instance, the right to liberty and security of person, if the person is wrongly channelled into the return procedure, or the right to asylum in case of a false match with a person not qualifying for protection.

As concerns alphanumeric data, in addition to the reasons for inaccuracies listed in [Section 3](#) affecting all data subjects, unaccompanied children, particularly when they are of younger age, may more commonly give incomplete or wrong information. This would affect the reliability of data entered in the system.

Preventing disproportionate effects of children's criminal records, including immigration law offences

In its opinion on the proposed upgrade of the European Criminal Records Information System (ECRIS) concerning the exchange of information on third-country nationals, FRA highlighted several elements that may have a disproportionate effect on children. This includes the impact on children of convictions related to migration

or trafficking in human beings, and the sensitivity of children's criminal records.⁹² These elements are also relevant in the context of interoperability given that the planned dedicated ECRIS for third-country nationals might be interoperable with other EU IT-systems.

Some children may have been compelled to commit offences as a consequence of being subject to trafficking in human beings, notably as a result of exploitation. Others may have criminal records relating to migration-related offences when they were moving together with their parents. Legislation criminalising irregular entry or stay varies among Member States,⁹³ and the existence of a criminal record may depend on where they have been apprehended. Children should not suffer disproportionate consequences for decisions made by their parents.

According to the United Nations (UN) Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules'), recalled also by the UN Convention on the Rights of the Child, records of juvenile offenders should be kept strictly confidential and closed to third parties, and should not be used in adult proceedings in subsequent cases involving the same offender.⁹⁴

4.2. Interoperability as a tool for child protection

Interoperability may also bring new opportunities to protect the rights of children. It could, for example, allow the authorities to intervene in the best interests of missing children. If a child who has been previously recorded in SIS II as missing is encountered by the authorities and checked against one of the other databases, the SIS II entry would be visible due to interoperability, allowing the authorities to take appropriate action.

Such a scenario would require that all missing children are systematically included in SIS II. At present, the SIS II Regulation does not oblige the Member States to register all missing children in SIS II. According to desk research undertaken by FRA in 2014, most Member States systematically create SIS II alerts for missing children, but in some the decision to introduce an alert is left to the local police. Police authorities can only register children who have been reported to them as missing by the responsible bodies, such as reception and asylum centres, and this does not systematically happen.

FRA's survey on biometrics among border guards in six Member States shows that children reported as missing are frequently encountered at border crossing points.

89 JRC Technical Repots (2014).

90 FRA (2016b), p. 26.

91 See for example Aashmi, Sakshi Sahni, Sakshi Saxena (2014); Ramanathan, N., Chellappa, R., Biswas, S. (2009).

92 FRA (2015b), pp. 21-22.

93 FRA (2014).

94 United Nations (1985), Rule 21.

In this survey, border guards were specifically asked how often they have encountered, during the previous 12 months, a case of a child with an alert in SIS II as a missing person. Almost a third of the border guards (29 %) experienced this at least 1-10 times over the 12 month period. Some respondents even indicated that it happened more than 10 times or even more than 50 times in the preceding year, as shown in Figure 3. If they were to encounter a child with a SIS II alert for missing persons, the majority of respondents would follow the general procedures of stopping the child and sending it for a second line check. Most of the respondents – but not all them – stated they would make an inquiry via the operational SIRENE (Supplementary Information Request at the National Entries) cooperation channels to their own Member State and the Member State that issued the SIS II alert. Other actions frequently taken by border guards are calling interpreters and handing the child over to the child protection authorities.

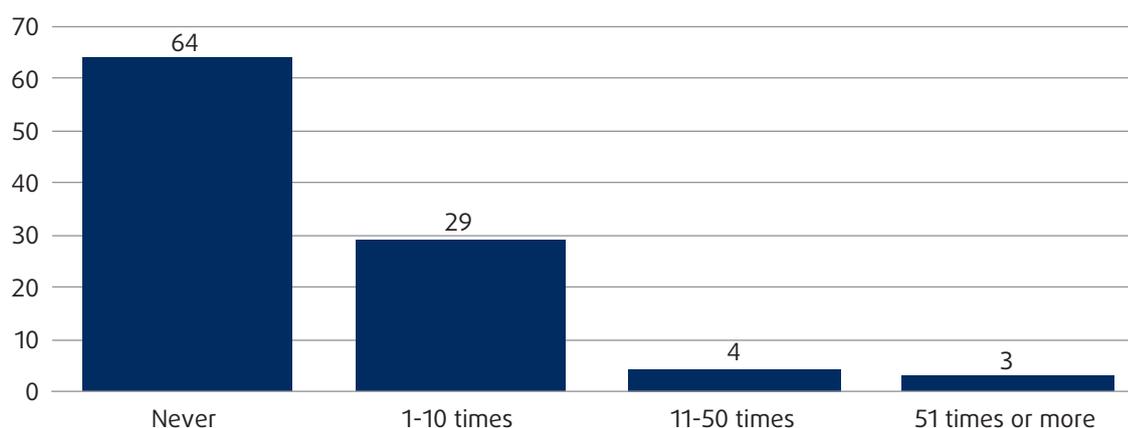
The quality and completeness of SIS II alerts is considered insufficient by many border guards. Border guards asked about the main problems encountered when using SIS II alerts for identifying missing children indicate that incorrect data are the most pressing problem. 62 % of border guards indicate that the data included in SIS II are sometimes incorrect or not updated. 41 % consider it a major problem that the personal data included in the SIS II alert are not sufficient to allow identification, if the child does not have a genuine travel document. More than a third (36 %) consider it a problem that not

all EU Member States issue SIS II alerts for every child reported missing.

To improve possibilities to detect missing children, some of them possibly victims of human trafficking, systematic recording of missing children in SIS II could be further interlinked with changes in other systems. In this context, synergies with Eurodac could be considered also given the planned reduction of age of children to be included in the system. For example, once a child is reported as missing, interoperability between Eurodac and SIS II could make the child's data from Eurodac available to authorities responsible for the prevention, detection and investigation of trafficking. This could be combined with a specifically defined child protection objective that would be added to the Eurodac Regulation to ensure that such access would be in line with the principle of purpose limitation, without unduly extending the availability of the data of all children.⁹⁵

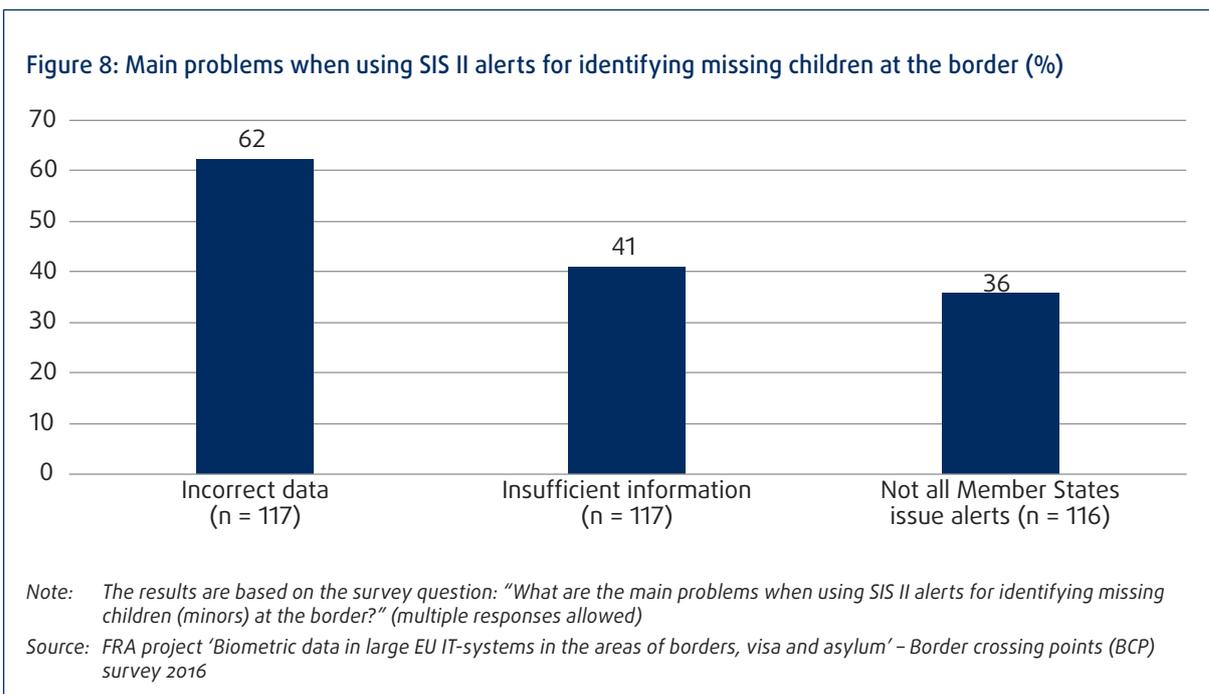
Increased availability of information does not in itself guarantee better protection of missing children or child victims of trafficking. Positive impact of interoperability on safeguarding the child's best interests would also require that clear follow up measures are in place. Such measures would include referral to child protection authorities, a needs assessment and the determination of a durable solution, together with any investigation which may be necessary if the child is a victim of serious crime. At the same time, persons who may encounter children in need of protection need to be in possession of adequate knowledge on how to respond

Figure 7: Estimated number of times border guards come across an SIS II alert of missing persons when dealing with children (%)



Note: The results are based on the survey question: "How often have you come across a child (minor) at this border who had a SIS II alert as a missing person? Please provide an estimated number of times when this has happened in the last 12 months..."

Source: FRA project 'Biometric data in large EU IT-systems in the areas of borders, visa and asylum' – Border crossing points (BCP) survey 2016



to such situations. This may require a new approach to training needs at the Member States' level. Inclusion of information on family links in the relevant IT-systems could then facilitate family tracing.

Conclusions

When it comes to the rights of children, interoperability brings additional challenges and opportunities. Some of the general risks are amplified in the case of children.

First, there is a higher risk of unreliable data being stored in IT-systems, compared to adults. Ongoing physical development of children may reduce the reliability of matches based on biometric data, particularly after a longer period. Matches based on fingerprints older than five years, or on a facial image, should therefore always be subject to further checks and be verified against other available data.

Second, information on criminal records may have a disproportionate impact on children – for example, due to immigration offences for which children cannot be held responsible. Particularly in case of a common repository, special conditions should apply to information on past criminal records contained in the European Criminal Records Information System (ECRIS). In light of the vulnerability of children, consideration should be given to either excluding information on criminal records of children from the scope of the interoperable solutions altogether or to limiting the availability of this information to very serious crimes committed by children.

Interoperability can nonetheless support the detection of missing children or children subject to trafficking in human beings, and facilitate a targeted response. This requires systematic recording of missing children, additional focus on child protection in the individual IT-systems, as well as functioning referral mechanisms and training of users who may encounter children in need of protection.



5

International protection



Under EU law, Article 18 of the EU Charter of Fundamental Rights protects the right to asylum. Effective access to international protection also forms the basis for the protection from *refoulement*, which is reflected in Article 19 of the Charter as well as Article 78 of the Treaty on the Functioning of the European Union.

Persons seeking international protection are generally considered to be in a vulnerable situation, due to the reasons that made them leave the country of origin, as well as the situation of uncertainty in which they find themselves in the host country. Eurodac, the information system that contains the data of all registered asylum seekers, therefore contains additional safeguards as compared to the other systems – for example, with regard to law enforcement access.

Through interoperability, identity fraud will be more easily identified. However, the use of false documents should not have an undue impact on protection-related decisions. In case of *Zh. and O.* before the CJEU, the Advocate General underlined that many individuals seek to hide their identity when fleeing their country of origin to protect themselves,⁹⁶ while others may be physically unable to obtain the documents necessary for legal entry (such as a passport and visa) when escaping from a conflict zone.⁹⁷

Notwithstanding the challenges linked primarily to privacy and data protection, interoperability of Eurodac with other databases may have certain beneficial effects, if accompanied by adequate safeguards. FRA research revealed cases where Eurodac was not

consulted and the return of persons who had applied for asylum in other Member States was carried out.⁹⁸ If an officer performing a check on a person in another database – for example, SIS II – would be immediately able to see that a person is a registered asylum seeker, this would help prevent further steps that may otherwise be initiated if the person is considered a migrant in an irregular situation. Interoperability could thus prevent apprehension, possible detention and return of asylum applicants, thus helping to uphold the principle of *non-refoulement*. It would also show the officer that since the person is an asylum seeker, his or her data should not be shared with third countries (particularly the country of origin) for the purpose of establishing the person's identity and obtaining travel documents. To make this possible, the selected interoperability solution would need to show that the person is an asylum seeker (rather than just having an entry in Eurodac). At the same time, access to additional data stored in Eurodac should be barred, if not permitted according to rules on authorised access.

Interoperability could also serve to provide information in the asylum procedure and facilitate access to international protection. Many persons arrive to the EU without travel documents, and while some deliberately destroy them, those fleeing persecution or armed conflicts are often forced to leave without travel documents, or lose them on their way to Europe. This is a complicating factor when establishing their identity and may lead to negative consequences, ranging from delays in the asylum procedure to undermining their actual chances to obtain international protection. If these persons have previously travelled to the EU, interoperability based on a biometric matching service can allow comparing their

96 CJEU, C- 554/13, *Z. Zh. and O. v Staatssecretaris van Veiligheid en Justitie*, opinion of Advocate General Sharpston delivered on 12 february 2015, para 63.

97 In relation to the non-penalisation of the use of fraudulent documentation and the applicable UNHCR standards, see for example FRA (2015b), p. 11.

98 Information provided by Slovak Humanitarian Council (provider of legal assistance to asylum seekers and refugees).

biometric data with those contained in other databases such as VIS or the EES, thus confirming their identity and avoiding negative consequences of the inability to produce valid travel documents.

At the same time, making IT-systems interoperable with those that are fed by non-EU Member States may involve fundamental rights risks. One example would be the Interpol Stolen and Lost Travel Documents Database (SLTD).⁹⁹ The SIS II proposal is expected to improve interoperability between the document section of SIS and the SLTD.¹⁰⁰ Member States need to be aware that third countries wishing to limit the possibilities of persons in need of protection, such as political opponents, may report the travel documents as stolen or lost to try to prevent the person from leaving.

As pointed out in [Section 2](#), interoperable systems may for a variety of reasons be particularly attractive to hackers. If information systems are not immunised against unlawful access by countries of origin, asylum applicants or their family members who remain in the country of origin may be exposed to acts of retaliation to force dissidents to return, hence undermining the right to asylum enshrined in Article 18 of the Charter.¹⁰¹

Interoperability may improve possibilities to identify protection needs and vulnerabilities. But technical failures, improper or insufficient use of the systems may limit such possibilities. If an IT-system informing about the need for protection cannot be consulted, this may lead to potential risks for the person concerned. FRA

research found that rather frequently VIS did not function as it should at borders. Only 10 % of border guards surveyed indicated that they have never experienced VIS not working.¹⁰²

Conclusions

Interoperability may have beneficial effects for persons seeking international protection. Ensuring that information about an asylum-seeker's status is visible when consulting IT-systems would reduce the risk of apprehension, detention or return. Past records in other systems may also help establish the identity of a person forced to flee persecution or other risk of harm without travel documents. However, information originating from third countries that may be consulted through interoperable systems should not be taken at face value, since oppressive regimes may include information about opponents to prevent them from leaving the country.

Interoperable IT-systems may be particularly prone to hacking and unauthorised access because of the large amount of information they hold, including about persons in need of protection. IT-systems holding such data need to be protected by robust data security measures, as well as administrative safeguards to prevent such intrusions. Similarly, safeguards would need to be in place to ensure that data are not unlawfully shared with third countries.

⁹⁹ Interpol (2017b); Interpol (2017a).

¹⁰⁰ European Commission (2016), COM(2016) 883 final, Brussels, 21 December 2016.

¹⁰¹ See FRA (2016b), pp. 31-33, and FRA (2016a), pp. 54-55.

¹⁰² FRA (2016), Biometrics BCP survey.



6

Risk of disproportionate effects on the rights of migrants in an irregular situation



Under international law and subject to their treaty obligations, including the European Convention on Human Rights, sovereign states are entitled to enforce immigration law and thus determine who can enter to, and stay on, the territory of the State. EU Member States must issue a return decision to migrants in an irregular situation under Article 6 (1) of the Return Directive or legalise them. Returning migrants requires that they are found. As demonstrated by FRA research on rights of migrants in an irregular situation, certain enforcement measures have a disproportionate impact on their ability to enjoy basic rights protected by the Charter.¹⁰³ This concerns rights such as the right to education (Article 14), the right to health care (Article 35) and the right to an effective remedy (Article 47), which must be provided to everyone, without discrimination.

Making the IT-systems interoperable will contribute to more efficient immigration law enforcement, as a number of IT-systems can simultaneously be accessed to determine if a person who has been stopped has the right to stay and to establish his or her identity. As Table 3 shows, the purpose of apprehension and return has been added to several EU IT-systems.

Interoperability is expected to contribute to more effective identification of irregular migrants and return. Migrants in an irregular situation would therefore avoid situations in which they risk apprehension. FRA research has shown that if migrants in an irregular situation know that they risk to be apprehended or reported to the authorities, they will be discouraged from approaching providers of basic services, such as medical facilities, or NGOs that offer legal advice, or from sending their children to school.¹⁰⁴ Migrants in an irregular situation who are victims of crime may be reluctant to approach

the police in fear that this would lead to their removal, which puts them at risk of further victimisation and allows perpetrators to remain unpunished. According to Recital 10 of the Victims' Rights Directive, the right of victims to be acknowledged as victims and to have access to justice should not be made conditional on their residence status. FRA research showed that victims of severe labour exploitation who are in an irregular situation of residence are discouraged by their status from reporting to any public authority. Experts identify fear of having to leave the country as the primary reason why victims do not report their exploitation to the police.¹⁰⁵ Victims of other forms of crime may have similar reasons not to report to the authorities.¹⁰⁶

Interoperability would increase the likelihood that law enforcement officers may be able to discern that a person reporting a crime (as a victim but potentially also a witness) is in an irregular situation. For example, if the officer consults SIS II or the future ECRIS database dedicated to third-country nationals and receives a notification from the Entry-Exit System that the person is an over-stayer, he or she may decide to inform the competent immigration authorities. This may further reduce the willingness of such persons to report a crime, driving them deeper underground without an effective access to justice. At the same time, it would deprive law enforcement authorities of the opportunity to effectively combat crime.

Conclusions

In general, an irregular migration status should not prevent persons from accessing basic services, such as healthcare or children's education, nor should persons

¹⁰³ FRA (2011).
¹⁰⁴ *Ibid.*

¹⁰⁵ FRA (2015c), p. 19.
¹⁰⁶ FRA (2011).

in an irregular situation be discouraged from seeking legal advice or reporting crime due to fear of being apprehended. An automatic notification of an irregular status when consulting databases would undermine this objective, as irregular migrants would avoid situations in which they may risk apprehension or being denounced to the immigration authorities. Therefore, FRA guidelines on apprehension of migrants in an irregular situation suggest that social service providers should not share information with immigration authorities. The guidelines also suggest that possibilities could be considered for victims and witnesses to report crime without fear of being apprehended.¹⁰⁷ Ensuring fundamental rights compliance of apprehension policies needs to be highlighted since interoperability is expected to result in making such policies more efficient.

¹⁰⁷ FRA (2012).



7

Risk of unlawful profiling when undertaking risk assessment



The data contained in IT-systems can be used for risk assessment or profiling. According to the General Data Protection Regulation, profiling is “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person”. The Council of Europe has defined profiling as a ‘computer method making use of data mining on a data warehouse, enabling or intended to enable the classification, with some probability – and thus with some margin of error, – of an individual in a specific category in order to take individual decisions towards that person.’¹⁰⁸ In the field of law enforcement, profiling can be used to flag persons against whom there is, or there is no, individual suspicion, so that these can be subjected to more detailed checks.

Both the General Data Protection Regulation and Directive (EU) 2016/680, which deals with the processing of personal data for criminal law purposes, are applicable in this context, depending on the purpose of processing. Article 22 (1) of the General Data Protection Regulation prohibits any “decision based solely on automated processing, including profiling” which “significantly affects” a data subject. Although exceptions may be made where authorised by EU or Member State law, data controllers must provide appropriate safeguards to data subjects including “the right to obtain human intervention [...], to express his or her point of view and to contest the decision.” The nature of other safeguards is not specified, but Articles 13 and 14 of the General Data Protection Regulation state that in case of profiling a data subject has the right to “meaningful information about the logic involved.” Article 11 of Directive (EU) 2016/680 prohibits profiling producing adverse legal effects for or significantly affecting the data subject,

unless authorised by law and accompanied at least by the right to a human intervention by the controller.

Furthermore, even if the risk assessment is carried out according to data protection safeguards, use of sensitive data listed in Article 9 of the General Data Protection Regulation is in principle prohibited. Sensitive data listed in Article 9 are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation is in principle prohibited. If these characteristics are used as the basis for profiling, there is a strong risk of discriminating against persons falling within these groups. This is because profiling relies on making assumptions about the way people behave based on a particular identifiable characteristic. Their use for profiling is exceptionally permitted where it is necessary for reasons of substantial public interest, on the basis of Union or Member State law.

Article 9 (2) (g) of the General Data Protection Regulation nevertheless requires that such law is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This means that the principles of purpose limitation, data minimisation and accuracy fully apply. According to Article 22 (4) “suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests” need to be in place. The same requirement is enshrined in Article 11 (2) of Directive (EU) 2016/680. Both instruments also require the data controller to conduct a ‘data protection impact assessment’ in the case of automated processing, including profiling, where the context and

¹⁰⁸ Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2008), pp. 3-4.

purposes of the processing is likely to result in a high risk to fundamental rights.

Even where the profiling is based on public interest stipulated in law, it will still be considered unlawful where it is discriminatory in nature, either directly or indirectly.¹⁰⁹ In the words of the Racial Equality Directive, discrimination occurs “where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin.”¹¹⁰ Direct discrimination would mean that the police would, for instance, stop members of an ethnic minority on suspicion of committing an offence solely or mainly because they are members of that ethnic minority. Indirect discrimination would mean that applying a rule that is neutral on the surface (e.g. search visa holders for the purpose of preventing or investigating crime) in practice mainly has a more negative impact on one particular ethnic, racial or religious group compared with other groups (e.g. if visa holders are mostly Africans and Asians). Article 11 (3) of Directive (EU) 2016/680 explicitly prohibits any profiling that results in discrimination on the basis of sensitive data. Automated risk assessment or profiling would, therefore, have to be based on algorithms that are not primarily or solely determined by personal characteristics that reveal sensitive information such as, race, ethnicity, health, sexual orientation, and religious beliefs.

Use of biometric data presents a specific challenge in the context of risk of discriminatory profiling. Facial images may reveal ethnic origin, but may also allow for automated ethnic classification. Some experts argue that fingerprints and the iris can also reveal ethnic origin and could be subject to automated ethnic classification.¹¹¹

The risk of discriminatory profiling increases if IT-systems are interoperable, as several data categories revealing sensitive data could be accessed simultaneously. By accessing several interoperable databases, data such as facial image, fingerprints, name, and country of origin could be used for profiling. In addition, according to Article 15 (4) (a) of the current proposal, ETIAS would include sensitive health-related information. Moreover, even where the data used to make the decision do not fall in the category of sensitive data, it could act as a proxy revealing the actual sensitive data.

At the same time, availability of additional information on which risk assessment can be based could have positive effects, allowing for more focused searches based on a combination of non-sensitive criteria instead of relying on few sensitive categories. In this manner,

interoperability could also help objectivise the way in which individual border guards, for example, assess individual passengers, and reduce the risk of discriminatory profiling due to prejudices or subjective attitudes.

Although the right of the data subject to information is a general principle applicable to the EU databases, the right to a ‘meaningful explanation’ about the underlying logic of the process, plays a specific role in relation to profiling.¹¹² It reflects the ‘black box’ nature of automated decision-making based on algorithms. In the absence of relevant jurisprudence, the exact scope of this right is yet unclear. The controllers nevertheless have to be prepared to outline the basic principles on which an individual decision has been made. This duty needs to be seen in combination with the requirement of Article 12 of the General Data Protection Regulation that communication with data subjects is in a concise, intelligible and easily accessible form.

In a situation of interoperability, this would require clarity on the origin of the individual data sets, and could lead to issues related to the correction and rebuttal of potentially incorrect information (see below).

Conclusions

Automated risk assessment needs to be based on algorithms that are not determined by data revealing sensitive information about a person. By increasing the availability of such information contained in individual databases, interoperability may increase the risk of discriminatory profiling. At the same time, access to additional information due to interoperability may help reduce the likelihood of discriminatory risk assessment based on sensitive personal data. Interoperability would allow conducting more focused searches based on a combination of non-sensitive criteria instead of relying on a limited number of sensitive categories.

¹⁰⁹ In this context, see FRA (2010).

¹¹⁰ Council Directive 2000/43/EC of 19 July 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180/22.

¹¹¹ Paul de Hert (2013), p. 391; Els J. Kindt (2013), p. 320.

¹¹² See for example Goodman, B., Flaxman, S. (2016).



References

- Aashmi, Sakshi Sahni, Sakshi Saxena (2014), 'Survey: Techniques for aging problems in face recognition', *MIT International Journal of Computer Science and Information Technology*, Vol. 4, No. 2, August 2014.
- Alterman, A. (2001), 'A piece of yourself: Ethical issues in biometric identification', *Ethics and Information Technology* (5).
- Anderson, D.Q.C. (2016), *Report of the Bulk Powers Review*.
- Article 29 Data Protection Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN, WP 169, Brussels, 16 February 2010.
- Article 29 Data Protection Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 203, Brussels, 2 April 2013.
- CJEU, C- 275/06, *Promusicae v. Telefónica de España SAU*, opinion of Advocate General Kokott delivered on 18 July 2007.
- CJEU, C- 554/13, *Z. Zh. and O. v Staatssecretaris van Veiligheid en Justitie*, opinion of Advocate General Sharpston delivered on 12 February 2015.
- CJEU, C-291/12, *Schwarz v. Bochum*, 17 October 2013.
- CJEU, C-362/14, *Schrems*, 6 October 2015.
- CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008.
- CJEU, C-73/07, *Satakunnan Markkinapörssi and Satamedia*, 16 December 2008.
- CJEU, C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, 9 November 2010.
- CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Secretary of State for the Home Department*, 21 December 2016.
- CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014.
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2007 L205/63 (SIS II).
- 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, OJ 2008 L210/1.
- 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, OJ L 218/129.
- Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ 2009 L 93/33.
- Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2008), *L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultative*, 11 January 2008.
- Council of the European Union (2016a), *Renewed Information management Strategy – draft 5th Action List*, 5175/3/16 REV 3, 27 June 2016
- Council of the European Union (2016b), *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area (2016)*, 9368/1/16 Rev 1, 6 June 2016.
- Decision No. 922/2009/EC of the European Parliament and of the Council of September 2009 on interoperability solutions for European public administrations (ISA).
- Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA² programme) as a means of modernising the public sector.
- ECTHR, *Djalo v. the United Kingdom*, No. 17770/10, communicated on 10 December 2014.
- ECTHR, *F.N. and Others v. Sweden*, No. 28774/09, 18 December 2012.
- ECTHR, *Gare-Simmons v. the United Kingdom*, No. 71358/12, communicated on 10 December 2014.

ECtHR, *Hall v. the United Kingdom*, No. 21457/11, communicated on 10 December 2014.

ECtHR, *I. v. Finland*, No. 20511/03, 17 July 2008.

ECtHR, *M.K. v. France*, No. 76100/13, 18 April 2013.

ECtHR, *Murphy v. the United Kingdom*, No. 51594/10, communicated on 10 December 2014.

ECtHR, *Osman v United Kingdom*, No. 87/1997/871/1083, 28 October 1998.

ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

EDPS (2008), *Opinion of 26 March 2008 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004*, OJ C 200, 6 August 2008.

EDPS (2010), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, 18 March 2010.

EDPS (2016), *EDPS Opinion on the Second EU Smart Borders Package*, Opinion 6/2016, 21 September 2016.

Els J. Kindt (2013), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, London, Springer.

Eu-LISA, (2015), *Smart Border Pilot Final Report: Report on the technical conclusions of the Pilot*, Volume 1.

European Commission (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, COM(2010) 245 final/2, Brussels 26 August 2010.

European Commission (2010), *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, 20 July 2010.

European Commission (2010), *Towards interoperability for European public services*, COM(2010) 744 final Brussels, 16 December 2010.

European Commission (2015), *A digital Single Market Strategy for Europe*, COM(2015) 192 final Brussels, 6 May 2015.

European Commission (2015), *A European Agenda on Migration*, COM(2015) 240 final, Brussels, 13 May 2015.

European Commission (2015), *The European Agenda on Security*, COM(2015) 185 final, Strasbourg, 28 April 2015.

European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)*, COM(2016) 272 final, Brussels, 2 May 2016.

European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No. 767/2008 and Regulation (EU) No 1077/2011*, COM(2016) 194 final, Brussels, 6 April 2016.

European Commission (2016), *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, Brussels 16 November 2016.

European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU*, COM(2016) 883 final, Brussels, 21 December 2016.

European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006*, COM(2016) 882 final, Brussels, 21 December 2016.

European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third country Nationals*, COM(2016) 881 final, Brussels, 21 December 2016.



- European Commission (2016), *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, COM(2016) 655 final, Brussels, 14 October 2016.
- European Commission (2016), *Communication from the Commission to the European Parliament and the Council: Stronger and smarter information systems for borders and security*, COM(2016) 205 final, Brussels, 6 April 2016.
- European Commission (2017), *European Interoperability Framework-Implementation Strategy*, COM(2017) 134 final, Brussels, 23 March 2017.
- European Commission (2017), *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/EC*, COM(2017) 8 final, Brussels, 10 January 2017.
- European Council of Refugees and Exiles (2013), *Bulgaria accused of putting asylum seekers at risk by providing information on Syrians to Syrian embassy*, Brussels.
- European Data Protection Supervisor (EDPS) (2017), *EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)*, Opinion 3/2017, 6 March 2017.
- FRA (2010), *Towards More Effective Policing, Understanding and preventing discriminatory ethnic profiling: A guide*, Luxembourg, Publications Office.
- FRA (2011), *Fundamental Rights of migrants in an irregular situation in the European Union: Comparative report*, Luxembourg, Publications Office.
- FRA (2012), *Apprehension of migrants in an irregular situation – fundamental rights considerations*, Working paper, Vienna 2012.
- FRA (2014), *Criminalisation of migrants in an irregular situation and of persons engaging with them*, Luxembourg, Publications Office.
- FRA (2015a), *Annual Work Programme*.
- FRA (2015b), *Opinion of the European Union Agency for Fundamental Rights concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information System*, 1/2015 [ECRIS], 4 December 2015.
- FRA (2015c), *Severe labour exploitation: workers moving within or into the European Union States' obligations and victims' rights*, Luxembourg: Publications Office.
- FRA (2016a), *Opinion of the European Union Agency for Fundamental Rights on the impact on children of the proposal for a revised Dublin Regulation (COM(2016)270 final 2016/0133 COD), 4/2016 [Dublin]*, Vienna, 23 November 2016.
- FRA (2016b), *The impact of the proposal for a revised Eurodac Regulation on fundamental rights. Opinion of the European Union Agency for Fundamental Rights, 6/2016 [Eurodac]*, 22 December 2016.
- FRA (2017), *The impact on fundamental rights of the proposal for a Regulation on the European Travel Information and Authorisation System (ETIAS). Opinion of the European Union Agency for Fundamental Rights*, 7 July 2017.
- FRA and Council of Europe (2014), *Handbook on European data protection law*, Luxembourg, Publications Office.
- Goncalves, M. E. and Gameiro, M. I. (2014), 'Does the Centrality of Values in the Lisbon Treaty Promise more than it can actually offer? EU Biometrics policy as a case study', *European Law Journal*, Vol. 20, No.1.
- Goodman, B., Flaxman, S. (2016), *European Union regulations on algorithmic decision-making and a "right to explanation"*, arXiv.
- Hallinan, D. (2015), 'Effects of surveillance on freedom of assembly, association and expression' in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, New York, Routledge pp. 268-270.
- High level Expert Group on Information Systems and Interoperability, *Register of Commission Expert Groups*.
- International Organization for Standardization (2011), *ISO/IEC 19794-5:2011 - Information technology - Biometric data interchange formats - Part 5: Face image data*.
- Interpol (2017a), *Border management: Fighting terrorism and transnational crime through effective border management: Systems*.
- Interpol (2017b), *Gestion des Frontieres: Stolen and Lost Travel Documents database*.
- JRC Technical Repots (2014), *Fingerprint recognition for children*, final report, Luxembourg, Publications Office.

Mordini, E., Green, M. (2009), Human rights, identity and anonymity: Digital identity and its management in e-Society. Identity, security and democracy.

Ramanathan, N., Chellappa, R., Biswas, S. (2009), 'Computational methods for modelling facial aging: A Survey', *Journal of Visual Languages and Computing* 20.

Paul de Hert (2013), *Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions*, In Patrizio Campisi (ed.), *Security and Privacy in Biometrics*, London, Springer.

Raab C. (2015), 'Surveillance: Effects on Privacy, autonomy and dignity' in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, New York, Routledge pp. 259-268.

Sanchez del Rio, J., Conde, C. et al., (2015), *Face-based recognition systems in the ABC e-Gates*, Department of Computer Science and Statistics, Rey Juan Carlos University, Madrid, Spain.

United Nations (1985), *Standard Minimum Rules for the Administration of Juvenile Justice* ('The Beijing Rules'), General Assembly resolution 40/33 of 29 November 1985.

Wikipedia, [View \(SQL\)](#).



Annex: Research methodology

Biometric data in large EU IT-systems in the areas of borders, visa and asylum – fundamental rights implications (2015-2017)

The FRA project on biometrics in large-scale European Union (EU) databases analyses the fundamental rights implications of collecting, storing and using biometric and other data in EU IT-systems in the fields of visas, borders and asylum. It examines both positive and negative fundamental rights implications of storing biometric and other data in Eurodac, SIS II (Schengen Information System) and VIS (Visa Information System).

The FRA research on biometrics in large-scale EU databases builds on a variety of research methods and data collection carried out in different phases between 2015 and 2016. The FRA paper Fundamental rights and the interoperability of EU information systems: borders and security draws on this research.

1. Franet research

FRA's multidisciplinary research network, Franet, carried out a mapping of relevant practices and procedures related to the use of databases in all EU Member States. The network partners in each Member State conducted desk research (review of available information) and contacted relevant authorities responsible for the data in the databases or its usage. Franet also assessed to which extent civil society is active and aware of the issues in this field.

2. Contracted field research

Fieldwork was carried out in 2016 at border crossing points (BCPs) in six EU Member States – Belgium, Germany, Italy, Poland, Spain and Sweden – and at a limited number of diplomatic missions and consular posts (DMCPs) in third countries. The countries were selected based on the different migration challenges they face, types of borders (mainly land and air borders) and geographical balance. Eticas Research and Consulting, and the Spanish Research Council (CSIC), Department of Demography carried out the fieldwork research on FRA's behalf. It included qualitative interviews, small-scale surveys and non-participant observations collecting information on the use of Eurodac, SIS II and VIS in the procedures for asylum, border checks, visa applications, apprehension of migrants in an irregular residence situation, responsibilities of controllers and supervisors of the data.

2.1. Qualitative interviews

The target groups for the qualitative interviews are experts, professionals and 'rights holders'. Professionals include persons whose work involves Eurodac, SIS II or VIS. These are data controllers for Eurodac, SIS II and VIS, national data protection authorities, border guards, police, asylum authorities, immigration authorities and staff responsible for processing of visa applications at the DMCPs (diplomatic missions and consular posts). The target groups further included lawyers and providers of legal assistance; they also included biometrics experts, IT experts and experts in the ethical, social and fundamental rights fields.

To collect the views and perspectives of right holders, such as asylum seekers, visa applicants, migrants in a regular or irregular situation, including both those apprehended at the border as well as inside the territory of a Member State, respondents were selected following quotas on age, gender and nationality by contacting associations dealing with these groups. A total of 286 semi-structured qualitative interviews were carried out following predefined interview guidelines and an interviewer training. With the consent of the interviewee, the interviews were recorded; otherwise, a reporting template was completed in English. FRA developed the interview questions which were available in English and the national languages of the Member States covered.

2.2. Small-scale surveys

Three surveys were carried out to collect information about experiences with the acquisition and use of biometric and other personal data at the border and for the visa application process. These surveys were conducted with

- (1) border guards (BCP survey);
- (2) staff processing visa applications at embassies and external service providers to embassies (DMCP staff survey);
- (3) visa applicants (visa applicants survey).

The FRA paper on Fundamental rights and the interoperability of EU information systems: borders and security builds on information from the BCP survey and the DMCP staff survey. FRA developed the questionnaires, which were available in English and the national languages of the Member State and the third country in question.

BCP survey

To explore the views and experiences of border guards, a small-scale survey among them was conducted at border crossing points (BCPs) in six EU Member States, including Zeebrugge port in Belgium (sea border), the airports Frankfurt in Germany, Barajas in Spain, Fiumicino in Italy and Arlanda in Sweden, as well as the border crossing point Terespol in Poland (train and road traffic). The fieldwork was carried out between June and October 2016, covering 160 respondents. The number of respondents per BCP varied, ranging from five border guards in Zeebrugge to 33 in Terespol.

The majority of border guards interviewed were men (72 %, with information on gender missing from 6 % of respondents). More than 60 % of the border guards surveyed have worked for more than three years as a border guard (27 % worked as border guards for more than 10 years) at the same BCP. Most border guards work as first-line officers (76 %), while 28 % work as second-line officers and 7 % as shift leaders. Twelve percent indicate to have another post, including other managers or coordinators, and assistants to the shift leaders.¹¹³

DMCP surveys

To capture the views and experiences of staff involved in the visa application procedure, a small-scale survey was carried out at embassies and external service providers to embassies (DMCPs) covering both staff (132 respondents) and visa applicants (584 respondents). The surveys were carried out in Algeria (at DMCPs of Belgium, Poland and Spain in Algiers), in Nigeria (at DMCPs of Belgium, Italy and Sweden in Abuja and Lagos), in Thailand (at the DMCPs of Germany, Italy and Sweden in Bangkok) and Ukraine (at the DMCPs of Germany, Poland and Spain in Kiev and Lviv). The selection of DMCPs was based on several criteria, including the following: staff being experienced with VIS, the overall number of visa

applications and the rate of rejections of applications; as well as a balanced geographical coverage.

The survey among staff working at DMCPs included 132 persons in four countries, Algeria, Nigeria, Thailand and Ukraine. The numbers per EU Member State ranged from 12 staff in Belgium up to 35 in Italy, and the number of staff interviewed per host country ranged from 15 persons in Algeria up to 53 in Nigeria. Sixty-two out of the 132 respondents worked for an external service provider.

Regarding the age distribution among respondents, more than half were aged 30 years or younger, and a quarter between 31 and 40 years. At 72 %, most of the respondents were female. Of the 584 visa applicants interviewed, 54 % were women and 43 % men; the remaining respondents did not provide any information on gender or selected the category 'other'. Regarding age, the sample of visa applicants was well balanced.

2.3. Non-participant observations

To contextualise better the results from the small-scale surveys, non-participant observations took place at the same locations where these were carried out. Non-participant observation is a qualitative data collection method in which the researcher observes events, activities and interactions to gain a direct understanding of a phenomenon in its context. The researchers adopt a more distant role and do not participate directly in the activities being observed (here processes of visa applications and border checks). The non-participant observations were made during the fieldwork for the small-scale surveys, which were conducted over one to two days. During the observations, researchers completed structured templates describing the activities observed, which were analysed afterwards.

¹¹³ The numbers do not sum up to 100 % because some respondents work in several positions, such as first and second-line officers.



HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:
from the European Union's representations (http://ec.europa.eu/represent_en.htm);
from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
by contacting the Europe Direct service (http://europa.eu/eurodirect/index_en.htm) or
calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

Various proposals on EU-level information systems in the areas of borders and security mention interoperability, aiming to provide fast and easy access to information about third-country nationals. When used to obtain information about individuals entering the EU, this implicates various fundamental rights set out in the EU Charter of Fundamental Rights, including to respect for private life and the protection of personal data. Adequate safeguards and mechanisms to ensure respect for these rights are thus essential. This publication aims to support the work of the high-level expert group on information systems and interoperability by highlighting ways to address fundamental rights challenges.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency



Publications Office

ISBN 978-92-9491-722-5