Council of the European Union

Brussels, 18 April 2018
(OR. en)

8037/18

Interinstitutional Files:
2017/0351 (COD)
2017/0352 (COD)

COSI 77	DATAPROTECT 62
FRONT 92	VISA 78
ASIM 38	FAUXDOC 24
DAPIX 105	COPEN 103
ENFOPOL 170	JAI 322
ENFOCUSTOM 69	CT 53
SIRIS 35	COMIX 189
SCHENGEN 11	CODEC 576

NOTE

From:	Mr Michael O'Flaherty, European Union Agency for Fundamental Rights
On:	17 April 2018
To:	Delegations
No. prev. doc.:	15119/17 + COR 1, 15729/17 + COR 1
Subject:	Interoperability and fundamental rights implications

Delegations will find attached the Opinion from the European Union Agency for Fundamental Rights on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

FRA Opinion – 1/2018 [Interoperability]

Vienna, 11 April 2018

Interoperability and fundamental rights implications

Opinion of the European Union Agency for Fundamental Rights

Contents

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA),

Bearing in mind the Treaty on European Union (TEU), in particular Article 6 thereof,

Recalling the obligations set out in the Charter of Fundamental Rights of the European Union (the Charter),

In accordance with Council Regulation 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (FRA), in particular Article 2 with the objective of FRA "*to provide the relevant institutions, bodies, offices and agencies of the Community and its EU Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights*",

Having regard to Article 4 (1) (d) of Council Regulation 168/2007, with the task of FRA to "*formulate and publish conclusions and opinions on specific thematic topics, for the Union institutions and the EU Member States when implementing Community law, either on its own initiative or at the request of the European Parliament, the Council or the Commission*",

Having regard to Recital (13) of Council Regulation 168/2007, according to which "*the institutions should be able to request opinions on their legislative proposals or positions taken in the course of legislative procedures as far as their compatibility with fundamental rights are concerned*",

Having regard to previous opinions of FRA on related issues; in particular the FRA opinion on the future European Criminal Records Information System for third-country nationals,[1] FRA opinion relating to the proposal for a revised Eurodac Regulation[2] and FRA opinion on the proposed Regulation on the European Travel Information and Authorisation System.[3]

Building on the mapping of fundamental rights implications of interoperability FRA published in July 2017 in the context of the work of the High Level Expert Group on Information Systems and Interoperability in the report 'Fundamental rights and the interoperability of EU information systems: borders and security'[4] as well as on the findings of the FRA research project on the processing of biometric data in large-scale information technology systems

---

1 European Union Agency for Fundamental Rights (FRA) (2015), *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*, FRA Opinion – 1/2015 [ECRIS], Vienna, 4 December 2015.

2 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016.

3 FRA (2017), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], Vienna, 30 June 2017.

4 FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017.

established by the European Union to manage asylum and migration published on 28 March 2018.[5]

Having regard to the request of the European Parliament of 28 March 2018 to FRA for an opinion "on the fundamental rights implications", among others on the right to the protection of personal data, of increased forms of interoperability, including access by law enforcement authorities and Europol to EU information systems".

SUBMITS THE FOLLOWING OPINION

[5] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018.

Acronyms

AFIS	Automated fingerprint identification system
CIR	Common Identity Repository
CJEU	Court of Justice of the European Union (CJEU is also used for the time predating the entry into force of the Lisbon Treaty in December 2009)
Convention 108	Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
DNA	Deoxyribonucleic acid
ECHR	European Convention on Human Rights
ECRIS-TCN	European Criminal Records Information System on Third Country Nationals
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EU	European Union
eu-LISA	European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	European Dactyloscopy
Europol	European Union Agency for Law Enforcement Cooperation
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
Interpol	International Criminal Police Organization
IT system	Information technology system
MID	Multiple-Identity Detector
PNR	Passenger Name Record
shared BMS	shared Biometric Matching Service
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TDAWN	Travel Documents Associated with Notices
TFEU	Treaty on the Functioning of the EU
The Charter	EU Charter of Fundamental Rights
VIS	Visa Information System

Introduction

This Opinion by the European Union Agency for Fundamental Rights (FRA) aims to inform the European Parliament position concerning legislative proposals on interoperability between EU information technology systems (IT systems) presented on 12 December 2017 and currently discussed by the EU legislators.[6]

The content of the two proposals is essentially the same. Therefore, in this Opinion, FRA treats them together. All references to proposed legal provisions relate to both instruments, except when otherwise specified. Among the legal provisions pointed out by FRA in this Opinion, Articles 55a, 55b and 55e, and Recitals 58 and 59 apply only to the proposed Interoperability Regulation on borders and visas.

The FRA Opinion analyses the implications of increased levels of interoperability for fundamental rights.

Core elements of proposed interoperability

The proposed regulations intend to achieve interoperability between IT systems through four different components:

- ✓ a **European Search Portal – ESP**, to allow competent authorities to search multiple IT systems simultaneously, using both biographical and biometric data;
- ✓ a **shared Biometric Matching Service – BMS**, to enable the searching and comparing of biometric data (fingerprints and facial images) from several IT systems;
- ✓ a **Common Identity Repository – CIR**, containing biographical and biometric identity data of third-country nationals available in existing EU IT systems;
- ✓ a **Multiple-Identity Detector – MID**, to check whether the biographical and/or biometric identity data contained in a search exists in other IT systems so as to enable the detection of multiple identities.

A central element of the proposals is the verification of the identity of those individuals whose data are stored in one of the underlying IT systems and the detection of people who fraudulently use different identities. To achieve this, the identity data on a person stored in any of the IT systems except SIS are moved from the individual system to a common data storage – the Common Identity Repository. Annex 1 illustrates the type of data concerned, which also include biometrics. Entries that refer to the same person are linked. In some way, the Common Identity Repository established by the proposals could be described as a database of identities, which if deemed necessary in future could also be used for purposes beyond those currently envisaged.

The Common Identity Repository is supplemented by a tool to discover if a person appears in more IT systems. Such Multiple-Identity Detector will browse through the personal data stored. When it finds (possible) multiple identities of a person, these identities are linked and the links are categorised by using different colours: white, green, yellow and red depending on the situation, as illustrated in Table 1. All yellow links are subject to a manual verification after which they will be categoried as white, green or red.

---

[6] The two proposals are essentially the same and references to proposed legal provisions relate to both instruments, except when otherwise specified. The proposals are the: *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final and the *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, COM(2017) 794 final.

Table 1: Colour coding in the Multiple-Identity Detector

Colour code	Type	Description	Verification
White link (Article 33)	Clear identity	Same or similar identity	Link is created automatically
		Multiple lawful identities	Link is created after manual verification
Yellow link (Article 30)	Unclear identity	The linked data share the same biometrics, but different identity data, or no biometrics but different identity data	Temporary colour coding until a manual verification is carried out
Green link (Article 31)	Confused identity	The linked data refer to two different persons who do not share biometrics but similar identity data	Link is created after manual verification
Red link (Article 32)	Identity fraud	The linked data share the same biometrics but different identity data, or no biometrics but different identity data	Link is created after manual verification

Source: FRA, 2018

FRA mapped the fundamental rights implications of some of the key elements of the interoperability concept in its report *Fundamental rights and the interoperability of EU information systems: borders and security*.[7] The Common Identity Repository (CIR) was not conceptualised in full detail at the time FRA published its report and the Multiple-Identity Detector (MID) was not yet on the table. Therefore, this FRA Opinion gives more attention to those components of interoperability that were not yet fully conceptualised at that time.

FRA's involvement in the High Level Expert Group on Interoperability of the European Commission enabled the agency to share its fundamental rights expertise before the legislative proposals were drawn up. This is a good practice as it allowed the European Commission to mitigate some of the possible negative implications on fundamental rights from the outset.

The FRA Opinion focuses on fundamental rights issues that have emerged from the agency's past research. It is not fully comprehensive and should be read together with the Opinion by the European Data Protection Supervisor (EDPS). The 2017 FRA report on interoperability assesses fundamental rights risk and opportunities of the concept of interoperability more broadly, whereas this FRA Opinion analyses those elements in the legislative proposals that may disproportionately affect fundamental rights.

The right to protection of personal data and the right to respect for private life

The proposed Interoperability Regulations interfere with the right to respect for private and family life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter).

These rights are not absolute and limitations can be justified, but they have to respect the requirements imposed by the Charter. Under EU law, any limitation on fundamental rights guaranteed by the Charter must comply, among others, with the principles of necessity and proportionality. To be in line with the requirements of Article 52 (1) of the Charter, 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

[7] FRA (2017), Fundamental rights and the interoperability of EU information systems: borders and security, Luxembourg, Publications Office, July 2017.

the essence of the right, and be proportionate.[8] Similar requirements are also imposed by the European Convention on Human Rights (ECHR). According to Article 8 (2) of the ECHR, any interference with the right to respect for private life has to pursue a legitimate aim, be in accordance with the law as well as necessary in a democratic society (proportionate).[9]

The two core principles of data protection are data minimisation and purpose limitation.

The principle of data minimisation is spelled out in Article 5 (1) (c) of the General Data Protection Regulation (GDPR). It requires that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Data minimisation refers to both the amount of data collected and the data processed.

The principle of purpose limitation provides that personal data may be processed only for specified purposes that must be explicitly defined. The principle is mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the GDPR. According to the GDPR, 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.[10]

Not all components of interoperability apply to the same set of IT systems. As Table 2 illustrates, the European Search Portal (ESP) encompasses more systems than the other components, including two Interpol databases that are not governed by EU law. The shared Biometric Matching Service (BMS) only applies to systems that process biometric data. A special technical arrangement is proposed for the Schengen Information System (SIS).

---

8 See also CJEU, C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 December 2008, para. 56; Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 9 November 2010, para. 77; Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 52; and C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, para. 92.

9 See ECtHR, *S. and Marper v. the United Kingdom*, [GC] Nos. 30562/04 and 30566/04, 4 December 2008.

10 CJEU, C- 275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, Opinion of Advocate General Kokott delivered on 18 July 2007, para. 53.

Table 1: IT systems covered by the four components of interoperability

	Eurodac	SIS*	VIS	EES	ETIAS	ECRIS-TCN	Europol databases	Interpol	
								TDAWN	SLTD
ESP	✓	✓	✓	✓	✓	✓	✓	✓	✓
BMS	✓	✓	✓	✓		✓			
CIR	✓		✓	✓	✓	✓			
MID	✓		✓	✓	✓	✓			

Note: *SIS is not directly covered by CIR and MID. SIS can be accessed either through the ESP, in which case the BMS is used for biometric searches, or through the national copy of SIS, in which case the national AFIS would be used for biometric searches. See European Commission, Impact assessment, SWD (2017) 473 final, pp. 41-42.*

See acronym lists at the beginning of the FRA Opinion for the full names of the abbreviations used in this table

Source: FRA, 2018

One of the central fundamental rights questions of the proposed Interoperability Regulations relates to the principle of purpose limitation. In this context, the proposals blur partly the boundaries between migration management and the fight against (serious) crime and terrorism.

The starting point of the proposals is that interoperability does not affect access rights to the data held in the underling systems. In other words, through interoperability an officer would not be authorised to see more data on an individual than what he or she can currently access. There are, however, some exceptions to this. Table 3 lists the situations in which interoperability would give access to more data than an authority is authorised to see under the legal instruments regulating the underlying IT systems.

Table 3: Authorities' access to additional personal data through interoperability

	Proposed articles	Authority having access to additional data	Additional data
Checks carried out for any public security or public policy reasons (as decided by Member States)	20	Any police officer who considers it necessary to check an individual, for example, for public order reasons or because of suspicions related to an offence or a crime, if authorised by national law	All identity data stored on the individual in the IT systems without flagging which system(s) contain it
Checks to enforce immigration law	20	Any police officer who considers it necessary to check where the person is stored in one of the IT systems to determine whether the person is lawfully staying or not	All identity data stored on the individual in the IT systems without flagging which system(s) contain it
Persons with a red link (identity fraud)	21 (2)	All authorities entitled to access at least one system	Identity data of the person subject to a red link stored in any of the six underlying systems and flagging which system(s) contains the data

Persons when a manual verification of the identity is required (yellow link)	21 (1), 29 (3) and 30 (2)	All authorities entitled to access at least one system when they create or update an entry, as they will need to categorise a link showed as yellow (unclear identity)	Identity data of the person subject to a yellow link stored in any of the six IT systems and flagging which system(s) contains the data
Checks for law enforcement purposes	22 (1)	Member State designated law enforcement authorities and Europol can query the CIR for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case, to see which IT systems include information on a specific person.	List of IT systems in which information on a person can be found.
Systematic check of applicants for international protection against SIS	27 (1) (d)	When a Eurodac entry is created or updated, the system will automatically alert the officer in case an applicant for international protection is recorded in SIS with a yellow or red link.	An asylum officer responsible for registration of claims is informed about the presence of an applicant in SIS, including yellow and red links.

Source: FRA, 2018

A careful analysis is called for to assess whether or not it can be justified to make these additional data visible to authorities who would otherwise not have access to these in light of the principle of purpose limitation enshrined in Article 8 of the Charter. While this is debatable for some of the cases listed in the MID (see Table 1), the broad access to personal identity data on an individual stored in one of the IT systems suggested in Article 20 entails a high risk that the data may be used for purposes that were not initially envisaged.

The proposed regulations foresee an increased role of national supervisory authorities established in accordance with the General Data Protection Regulation (GDPR),[11] namely the national Data Protection Authorities. This is an important element that this FRA Opinion proposes to enhance further to ensure the lawfulness of the processing of personal data. The proposals do not, however, sufficiently clearly reflect the budgetary implications of this increased role resulting from the need for additional resources.

Impact on other fundamental rights

In addition to the obvious implications on the right to respect for private and family life (Article 7 of the Charter) and on the right to protection of personal data (Article 8 of the Charter), the proposed regulations affect a number of other rights guaranteed by the EU Charter of Fundamental Rights. Except for the right to non-discrimination to which the proposals dedicate a separate article, the proposed texts give little visibility to other fundamental rights they affect – in particular: the right to asylum guaranteed in Article 18 of the Charter; the protection in the event of removal, expulsion or extradition (Article 19 of the Charter); the rights of the child (Article 24 of the Charter); and the right to an effective remedy and to fair trial (Article 47 of the Charter).

Next to the immediate fundamental rights concerns resulting from the proposals, there are also possible longer-term implications of interoperability. The legal and technical solutions that regulate interoperability will constitute the basis for future developments. Although it is not yet on the table, the European Commission indicated that decentralised EU systems –

[11] 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 2016 L 119/1.

such as those operating under the Prüm framework[12] and the Passenger Name Record (PNR)[13] – may at a later stage be included in one or more of the interoperability components, should its necessity be demonstrated.[14] Therefore, the design of interoperability must already now take into account any possible future expansion of the set of data covered and its potential impact on fundamental rights.

Although not yet on the table for the EU, in the longer-term, particular as face-recognition technology develops, it is also conceivable that it will be technically possible to match faces recorded on videos taken from surveillance cameras – installed, for example, at the entrance of a shopping mall – against biometric pictures stored in IT systems.[15] In future, authorities may wish to seize this opportunity to combat irregular migration, crime and/or terrorism. This would raise very serious and new necessity and proportionality questions.

Finally, the interoperability proposals have been issued at a time when the legal framework of the majority of the affected information systems is under preparation or revision – this applies to the ongoing revision of Eurodac and SIS, and preparation of the future ECRIS-TCN[16] and ETIAS.[17] This means that the overall legal clarity as to the rules and safeguards applicable to the individual EU information systems is limited, which affects the possibility to objectively assess the full impact of the current proposals on fundamental rights and calls for strong *ex post* evaluations, as suggested in Section 6 of this FRA Opinion.

The FRA Opinion contains 28 individual opinions, addressing the following points:

- General fundamental rights safeguard clause
- Objectives of interoperability
- European Search Portal
- Shared Biometric Matching Service
- Multiple-Identity Detector
- Reporting and statistics
- Right to information
- Right of access, correction and deletion
- Mainstreaming fundamental rights in implementation

---

[12] 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 was integrated in EU, and the implementing Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/12 transposed into EU legal framework the basic elements of a 2005 international agreement between several EU Member States. The Prüm mechanism allows the automated comparison of fingerprints, DNA (in both cases on a hit/no-hit basis) and vehicle registration information.

[13] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 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 (*PNR Directive*).

[14] European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final, 12 December 2017, Explanatory Memorandum, p. 5.

[15] See for example: http://www.anyvision.co/index.php/2018/02/08/nvidia/

[16] 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 (2017), *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information system (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011*, COM(2017) 344 final, 29 June 2017 (*ECRIS-TCN proposal*).

[17] 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 (*ETIAS proposal*).

1. Non-discrimination and a general fundamental rights safeguard clause

General fundamental rights and data protection safeguard clause

The proposed regulations contain a non-discrimination safeguard clause in Article 5. However, the operative parts of the draft regulations do not contain a general fundamental rights clause, which can only be found in the recitals. Recital 77 of the visas and borders proposal and Recital 68 of the police and judicial cooperation, asylum and migration proposal note that the regulations "respect fundamental rights and observe the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles." Recitals 48 of both proposals indicate that the EU data protection acquis – meaning Regulation (EU) 2016/679 and Directive (EU) 2016/680 – apply. Placing these provisions in the operative part of the regulations would better promote a fundamental-rights sensitive implementation.

Equality before the law and non-discrimination

Article 21 of the EU Charter of Fundamental Rights provide for freedom from discrimination. The general principle of equal treatment in Article 20 of the Charter requires that "comparable situations are not to be treated differently and [that] different situations are not to be treated alike unless such treatment is objectively justified".[18] Furthermore, where an apparently neutral rule disadvantages a person or a group sharing the same characteristics, a case of indirect discrimination occurs.[19]

Depending on the way it is designed and implemented (including the development and use of algorithms), interoperability can lead to differentiated treatment of people based on their sex, race, colour, disability or other grounds prohibited by the non-discrimination clause in Article 21 of the Charter.

This FRA Opinion will, therefore, analyse the impact of interoperability on the right to non-discrimination. The first section deals, more generally, with the proposed non-discrimination safeguard clause in Article 5 of the proposals, whereas subsequent sections deal with specific aspects of the proposals (see Sections 6 and 10).

The risk of discrimination is highest with the Multiple Identity Detector, which needs to be carefully assessed from different perspectives. The first one relates to sex. Women more frequently change their last name than men. In many countries, when a woman marries she takes on the family name of her husband. A woman who is in an IT system with her pre-marriage name and travels again will feature as a person having two different identities. The impact of the change of surname will depend on how sophisticated the algorithm for the automatic verification of multiple identity is. Nevertheless, statistically, women will remain more likely to be stopped at first entry compared to men (for example, where in addition to their surname other pieces of information such as passport details following a renewal of the document do not match) with the risk of missing connecting flights or other important commitments. This risk is higher where biometrics are not used, as is the case in ETIAS and partly in SIS, as searchable biometrics are only now gradually being introduced in SIS.

Also other groups of individuals – for example people from societies where certain names are very frequent (e.g. Mr/Ms Lee; Mohammed; etc.) – are likely to face more problems than

[18] CJEU, C-203/86, *Kingdom of Spain v. Council of the European Union*, 20 September 1988, para. 25 and CJEU, C-15/95, *EARL de Kerlast v. Union régionale de coopératives agricoles (Unicopa) and Coopérative du Trieux*, 17 April 1997, para. 35.

[19] FRA (2018), *Handbook on European non-discrimination law, 2018 edition*, Luxembourg, Publications Office, February 2018, p. 53.

others when their identities are verified. Without knowing the content of the future algorithm, the passenger flows and other variables, it is difficult to predict which categories of people the Multiple-Identity Detector will disproportionately affect in practice. Only an ex post evaluation will make it possible to assess the impact of interoperability on the right to non-discrimination in a comprehensive manner (see Section 10).

Persons who as a reflection of their social origin make mistakes when they complete an ETIAS request from their homes are one category who is likely to face more problems. A comprehensive non-discrimination provision in Article 5, which also covers the prohibition of discrimination based on "social origin" would help in making operators aware of possible risks of discrimination and also align this provision with Article 21 of the Charter.

The risk of unfavourable treatment may also originate from an unreliable biometric match. In case of facial recognition, phenotypical origin – thus the colour of the skin – plays also a role, as white skin reflects light more than dark skin and not enough illumination for very dark skin may result in false match.[20] Colour is included among the discrimination grounds in Article 21 of the Charter, but it is not reflected in Article 5 of the proposal. A safeguard is included in Article 13 (3), as biometrics stored in the individual IT systems have to meet minimum quality standards before templates are extracted and stored. Such standards could be set to mitigate the risk for an unreliable match, based on phenotypical origin.

Special attention for certain categories of people

Next to non-discrimination, interoperability may bring unforeseen negative consequences for children, older persons and persons with disabilities. Persons with disabilities enjoy the "freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice", in line with Article 21 of the Convention on the Rights of Persons with Disabilities.[21] The fact that they are not able to provide fingerprints making thus a comparison based on biometrics not possible, should not result in disadvantageous treatment.

The reliability of a fingerprint (but also a facial image) match decreases when fingerprints taken at a young age are compared many years after the time they were collected. With age fingertips also deteriorate which may affect the reliability of a match.[22] Most IT systems have a retention time of five years which helps reduce the risk of wrongful biometric matches. This is, however, not the case of Eurodac where data of applicants for international protection can be stored for up to 10 years.[23] The last sentence in Article 5 of the proposals – whereby particular attention must be paid to children, the elderly and persons with a disability – is, therefore, an important horizontal safeguard to remind the user to be particularly attentive when searches and identity verification procedures concern young people, the elderly or persons with disabilities. Implementing acts and eu-LISA could build on it. For example, eu-LISA, the Agency entrusted with ensuring data quality could promote

---

[20] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 90.

[21] United Nations (UN) (2006), Convention on the Rights of Persons with Disabilities, 13 December 2006.

[22] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 109.

[23] Regulation (EU) No. 603/2013 of 26 June 2013 on establishment of Eurodac (recast) OJ 2013 L 180/1 (*Eurodac Regulation*), Art. 12 (1); 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, 4 May 2016 (*Eurodac proposal*), Art. 17 (1).

the use of pop-up alerts, to prevent that matches that have a higher risk of being false than is normally the case are subject to rigorous manual verification, such as fingerprints of young children compared several years later.

Finally, through interoperability an increasing number of authorities will be able to access identity data stored in Eurodac, for example, to verify a yellow link or during a police check under proposed Article 20. As access points to the interoperable systems increase, so does the risk that an officer may share consciously or unintentionally information with a third party or country on the fact that an individual's data are stored in Eurodac. Although the proposed Article 48 prohibits the sharing of data stored in any of the interoperability components with any third country, international organisation or private party, the legal instruments regulating the underlying IT systems may allow it under certain conditions. In case of asylum applicants, such information would not only infringe on the privacy of the person concerned. It may also endanger his or her safety or the safety of family members remaining in the third country, thus undermining the right to asylum in Article 18 of the Charter. Interoperability will make access to data easier and, therefore, increase the risk that data are unlawfully shared with third countries. A general safeguard clause referring to the right to asylum would mitigate this risk.

FRA opinion 1

Despite the fact that the interoperability proposals also affect other fundamental rights, a general clause in the operative part of the regulations referring to the duty to apply the instruments in accordance with the rights and principles set forth in the Charter is missing. There is also no specific reminder to the right to protection of personal data in Article 8 of the Charter. Article 5 of the proposals contains an important safeguard clause on non-discrimination which, however, is phrased in rather limited way.

The EU legislator should, therefore:

- ***rename Article 5 to "Fundamental rights", thus reflecting the fact that interoperability may impact on a variety of rights enshrined in the EU Charter of Fundamental Rights;***
- ***add a first paragraph according to which "This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles.";***
- ***add a horizontal data protection safeguard clause to pay particular attention to ensuring that processing of personal data for the purposes of the proposed regulations do not result, either directly or indirectly, in undue interferences with the right to respect for private and family life, and the right to protection of personal data;***
- ***add "social origin" as well as "colour" to the grounds for non-discrimination listed in Article 5;***
- ***include "persons in need of international protection" among the groups of persons to whom particular attention should be paid in the implementation.***

2. Objectives of interoperability (Article 2)

The two proposals describe the objectives of interoperability in Article 2, with Recitals 9 and 10 providing further clarifications. FRA would like to provide two comments in this regard.

Protecting unaccompanied children who go missing

In its past opinions and reports, FRA has repeatedly underlined that IT systems – if accompanied by other measures – could help detect and protect child victims of trafficking as well as trace and better protect unaccompanied children who go missing, abscond or otherwise disappear.[24] However, neither Article 2 nor the Recitals make any reference to the use of interoperability for child protection purposes. Article 2 (1) of the two proposals establishes the objectives of interoperability by referring to the purposes of the single IT systems. Pursuant to Article 2 (1) (b) and (c), this includes also the objectives to contribute "to preventing and combating irregular migration" and "to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States".

In most cases, unaccompanied children who go missing from a reception facility are already registered in Eurodac with their fingerprints. When they disappear, they should be registered as missing persons in SIS – although in practice gaps remain as reception facilities do not always announce to the police that a child has disappeared and the police does not systematically register them in all EU Member States.[25] One can assume that, in most cases, the data used to register a missing child in SIS will be those given by the manager of the reception facility, which would normally correspond to the data contained in Eurodac (which will process also alphanumeric data once amended).[26] In future, interoperability between Eurodac and SIS will make it possible to link the two entries. Once the missing child is found, a biometric search will enable the police to link the child to the initial Eurodac registration as well as to the SIS alert.

The data recorded in Eurodac and SIS, including when the child went missing should not only be used to enforce immigration law but also be shared with the guardian and, in case return is envisaged, with the "appropriate body" referred to in Article 10 (1) of the Return Directive (2008/115/EC). Such information, is, of utmost importance for a proper assessment of the best interests of the child, as required by Article 24 of the Charter. However, if strictly interpreted, Article 2 (1) of the proposals could be read as preventing the sharing and use of past information on the child for the purposes of assessing the child's best interests. A clarification in a Recital could avoid such a strict interpretation.

---

24 See for example: FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, pp. 5, 6 and Section 2.2; FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017, p. 8 and Section 4.2; FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 12, Section 3.4, Section 7.6.

For a more detailed analysis on missing children, see Cancedda, A., Day, L., Dimitrova, D. and Gosset, M. (2013), *Missing children in the European Union, Mapping, data collection and statistics*, Study prepared for the European Commission, Luxembourg, Publications Office of the European Union.

25 See in this context also European Commission, The protection of children in migration, Brussels, 12 April 2017, COM(2017) 211 final, Section 3 which recommends "putting in place the necessary procedures and protocols to systematically report and respond to all instances of unaccompanied children going missing."

26 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 116.

Unaccompanied children who go missing are at heightened risk of exploitation and fall prey, in some cases, to criminal networks. Assuming that in many cases a missing unaccompanied child is registered in Eurodac and SIS, interoperability should maximise the use of such information to ensure that the child enjoys the right to such protection and care as is necessary for his/her well-being. This is an obligation deriving from Article 24 of the Charter.

FRA opinion 2

In principle, the interoperability proposals – read together with the pending revisions of SIS and Eurodac – offer new opportunities to reconstruct more objectively the history of an unaccompanied child who went missing.

The EU legislator should include a new Recital in the proposals referring to the use of interoperability for child protection purposes. In view of strengthening the protection of unaccompanied children, upon the identification of a missing child, such a Recital should recommend that EU Member States should promptly contact the child's guardian as well as relevant national child protection authorities. They should undertake a needs assessment with a view to finding a sustainable solution for the child in accordance with his or her best interests as required by Union and/or national law.

Keeping higher safeguards for more sensitive data

The proposals indicate that the objectives of interoperability will be achieved through various measures including "strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems" – Article 2 (2) (e). What strengthening and simplification mean is not obvious. On the contrary, in practice, as described in Section 9, the proposals will make the exercise of at least some data protection rights more complex for data subjects.

The currently existing differences in data protection safeguards are justified by the different sensitivity of the information contained in the various IT systems. Eurodac, for example, contains data on asylum applicants and refugees. The ECtHR considers asylum seekers as vulnerable.[27] Similarly, information on criminal records which will be stored in ECRIS-TCN are sensitive, as the knowledge of a past criminal record may consciously or unconsciously impact on the decision an officer may take relating to the person. This is in particular the case where Member States store and share criminal records of children, which under human rights law should be kept strictly confidential, so as to give children a realistic opportunity of rehabilitation and social reintegration.[28]

FRA opinion 3

The proposals say that interoperability will simplify data protection rules in the different underlying IT systems and make them more uniform. This implies a risk to disregard the different levels of sensitivity of the data stored within these systems. ECRIS-TCN data and data on applicants for international protection in Eurodac are particularly sensitive and thus deserve additional safeguards.

The EU legislator should therefore change the wording of proposed Article 2 (2) to reflect the different levels of sensitivity of data stored in the single IT systems. One possibility could be to rephrase Article 2 (2) (e) as follows: "Strengthening and simplifying data

---

[27] See for example, ECtHR, *M.S.S. v. Belgium and Greece*, [GC] No. 30696/09, 21 January 2011, para. 251; ECtHR, *A.S. v. Switzerland*, No. 39350/13, 30 June 2015, para. 29 (confirming the position in *M.S.S* under general principles).

[28] See Council of Europe (1984), Committee of Ministers, *Recommendation on the Criminal Record and Rehabilitation of Convicted Persons*, No. R(84)10, 21 June 1984, Section I. (5), and United Nations (1985), *Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules')*, General Assembly resolution 40/33 of 29 November 1985, Rule 21.

security and data protection conditions that govern the respective EU information systems, without prejudice to the special protection and safeguards afforded to certain categories of data".

3. European Search Portal (ESP)

The European Search Portal will allow competent authorities to search multiple IT systems simultaneously, using both biographical and biometric data. FRA has already shared its considerations on the impact of the European Search Portal on fundamental rights in the context of the HLEG Interoperability, which are to a significant degree addressed in the proposals.[29] Nevertheless, two issues remain.

Clarifying access rights

The European Search Portal must be designed in a manner which would ensure that a search launched by an officer only queries the IT systems that same officer is authorised to access in line with access rules as laid down in the respective legal instruments. Otherwise, it would violate the principle of purpose limitation mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the General Data Protection Regulation.

The current wording of Article 9 of the proposals is ambiguous and could lead to different interpretations. In Article 9 (1) the wording "in accordance with the user profile and access rights" is connected to the search launched by the officer instead of being related to the response he or she receives. The last sentence of Article 9 (6) seems to suggest that "where necessary" the officer could have access to additional information beyond what the officer is authorised to see.

FRA opinion 4

The unclear wording of proposed Article 9 could lead to different interpretations, bearing a risk of it being implemented in a way that is not in accordance with the principle of purpose limitation.

To ensure compliance with the principle of purpose limitation, the EU legislator should adjust the wording of Article 9 (1) to make clearer that a search launched by an officer only queries the systems he or she is authorised to access. In addition, the last sentence of Article 9 (6) should be deleted.

Mitigating risks for persons in need of international protection

The European Search Portal also queries two Interpol databases. Interpol administers a database on Stolen and Lost Travel Documents (SLTD) and a database on individuals who are subject of an Interpol alert (for example, a red notice to seek the location and arrest of a wanted person) – the Interpol Travel Documents Associated with Notices database (TDAWN).[30] SLTD and TDAWN are included in searches carried out through the European Search Portal.

Interpol databases are fed by information provided by national police authorities. In spite of Interpol's checks to exclude alerts based on political, military, religious or racial reasons, regimes in third countries may manage to include an alert on one of their nationals or on a document held by that person in the Interpol database to prevent the person from travelling or to find out where the person is hiding.[31] To shield the person and his/her family members

---

[29] FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017; High-level expert group on information systems and interoperability (2017), Final Report, Ref. Ares(2017)2412067, May 2017, Annex 3.

[31] For more information, see: https://www.interpol.int/About-INTERPOL/Legal-materials/Neutrality-Article-3-of-the-Constitution.

[31] For more information, see: https://www.interpol.int/About-INTERPOL/Legal-materials/Neutrality-Article-3-of-the-Constitution.

in the country of origin from protection risks, including a risk of kidnapping, interoperability queries to the Interpol databases must be adequately designed.

A safeguard for persons in need of protection is built into Article 9 (5) of the proposals. This provision states that data used to launch a query carried out through the European Search Portal will not be shared with the owners of Interpol data, thus the third country concerned. It is, however, unclear what the scope of the restriction is. If Article 9 (5) only concerns the data used for the query itself, but the owner of the data sees that data were consulted and by which national authority, this could expose an asylum applicant to protection risks as it would inform the country of origin of the whereabouts of the person. Particularly when such queries are launched from geographically smaller EU Member States, information about the authority launching the query can reveal sufficient details of the whereabouts of a person to put him or her at risk.

While this risk is to some extent already present now, when an authority consults the Interpol databases in a targeted manner, the proposed systematic verification of an individual subject of a European Search Portal query against the Interpol databases amplifies this risk.

FRA opinion 5

When the data of persons in need of international protection are queried against Interpol databases, there is a certain risk that information about the presence of an asylum applicant or a refugee becomes exposed to the country of origin, putting the individual or his/her family members at a heightened risk when fleeing regimes that have persecuted them.

The EU legislator should design interoperability in a way that – while respecting the legal framework regulating Interpol – the data owner would not receive any information that their databases have been queried through the European Search Portal, at least for those individuals who are registered in Eurodac as asylum applicants.

4. Biometric Matching Service (BMS)

The shared Biometric Matching Service would enable the searching and comparing of biometric data (fingerprints and facial images) from several IT systems. It is a tool to facilitate searches through the European Search Portal.

In practice, the EES[32] will by far constitute the greatest volume of new biometric data. Therefore, the basis of the shared Biometric Matching Service will de facto be established with the creation of the new EES. Biometric data from the other systems will be added by migrating the data contained in the SIS automated fingerprint identification system (AFIS), the Eurodac AFIS and the data of ECRIS-TCN into the shared Biometric Matching Service. The European Commission indicated 2023 as the due date for completion.[33]

This Section reviews the necessity of processing palm prints and DNA, examines access rights to the shared Biometric Matching Service and its data retention rules.

Excluding the processing of palm prints and DNA

The shared Biometric Matching Service will store the biometric templates that it obtains from the underlying IT system, according to Article 13 (1). All automated fingerprint identification systems (AFIS), including those currently used for Eurodac, the VIS and the SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples (Recital 17).

The biometric data to be stored under Article 13 go beyond the definition of biometric data included in Article 4 (12), which only refers to fingerprints and facial image, including also DNA and palm prints:

DNA: According to Article 13 (1) (d) of the proposed Interoperability Regulations – which refer to Article 20 (3) (x) of the SIS proposal on police and judicial cooperation – the shared Biometric Matching Service would also include DNA.

Palm prints: Article 13 (1) (c) as well as Article 13 (1) (e) propose that data referred to in Article 20 (2) (x) of the SIS proposal on border checks[34] and Article 4 (3) (u) of the SIS proposal on return,[35] should be part of the shared Biometric Matching Service. The SIS proposals on police and judicial cooperation (Article 3 (1) (l)) and the SIS proposal on border checks (Article 3 (1) (n)) define dactylographic data to encompass also palm prints.

Among the IT systems which will be made interoperable, only SIS contain DNA and palm prints, and they can be collected in certain situations only.

---

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

33 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final, 12 December 2017, Legislative Financial Statement, p. 82.

34 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 (*SIS II proposal (border checks)*).

35 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 (*SIS II proposal (return)*). The reference should read Article 4 (u).

FRA opinion 6

The purpose of the shared Biometric Matching Service is to identify a person across interoperable IT systems. Searches using DNA and palm prints will not help establishing links between identities stored in the different systems, because this sensitive data are only processed in SIS under certain conditions and not in any of the other systems. Considering also the high sensitivity of this information, their processing in the shared Biometric Matching Service would therefore not be necessary and proportionate, and conflict with the principle of data minimisation.

The EU legislator should, therefore, amend Article 13 (1) by deleting from Paragraph (1) (d) the reference to Article 20 (3) (x) of the SIS proposal on police and judicial cooperation, since this refers to DNA.

Moreover, with regard to Article 13 (1) (c)-(e) the EU legislator should clarify that the references to dactylographic data in SIS should only include fingerprints and not palm prints.

Better clarifying access rights

FRA understands that an officer who launches a query in the interoperable systems using fingerprints will only be able to see whether there is information stored on the individual in those systems he or she is authorised to access. This should be the case because the proposed Interoperability Regulations do not change access rules and data processing requirements of the individual IT systems. Nevertheless, to avoid diverging interpretations, the proposed regulations could be more explicit in this regard.

Pursuant to Article 13 (2), each biometric template will include a reference to the information systems in which the corresponding biometric data are stored. If such reference is visible to an officer undertaking a query, the simple knowledge that more information 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. Such hints may influence the decision an officer takes in relation to that individual.

FRA opinion 7

Article 8 (2) of the Charter, as well as Article 5 (1) (b) of the GDPR and Article 4 (1) (b) of the Police Directive,[36] set out the principle of purpose limitation. This principle requires that personal data are processed only for specified purposes, which must be explicitly defined. An officer who launches a search through the European Search Portal when implementing the shared Biometric Matching Service should only be able to access information he or she is authorised to see.

The EU legislator should add a sentence to Article 13 (2) clarifying that an officer launching a query using the shared Biometric Matching Service will see only the references to those information systems that he or she is authorised to access.

Strengthening data retention rules

According to the principle of storage limitation, as is expressed in Article 5 (1) (e) of the GDPR and Article 4 (1) (e) of the Police Directive, data that identify a data subject must

[36] 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 2016 L 119/89 (*Police Directive*).

not be retained for longer than is necessary for the purposes for which the data are processed. The data must be erased when the purpose has been served and there is no longer a justifiable reason to store them. The principle is also found in Article 5 (e) of Council of Europe Convention No. 108.

According to Article 15, data are stored in the shared Biometric Matching Service for as long as the corresponding data are stored in the Common Identity Repository and SIS. Article 23 regulates data retention for the Common Identity Repository indicating that the data stored therein must be deleted in accordance with the data retention provisions in the individual IT systems. Article 15, however, does not require that such data be "automatically" deleted, which is an important safeguard to ensure respect for data retention rules in practice.

FRA opinion 8

Article 15 of the proposals regulates data retention for the shared Biometric Matching Service and Article 23 regulates it for the Common Identity Repository. To ensure compliance with data retention rules, the EU legislator should require that all data stored in the shared Biometric Matching Service need to be automatically deleted as soon as the data retention time as regulated in the individual IT systems expires.

The EU legislator should include the word "automatically" in Articles 15 and 23 of the proposals dealing with the deletion of stored data.

5. Common Identity Repository (CIR)

Chapter IV of the proposals regulates the Common Identity Repository. It will contain biographical and biometric identity data of third-country nationals available in the following EU IT systems: Eurodac, VIS, EES, ETIAS, and ECRIS-TCN. SIS is not included in the Repository but can be accessed simultaneously through the European Search Portal.

The data stored in a common identity file will still 'belong' to the underlying systems. The Common Identity Repository will include a reference to the source system, as clarified in Article 18 (2).[37]

FRA understands that access to the Common Identity Repository through a search launched using the European Search Portal to consult an individual IT system is regulated in the legal instruments establishing those systems. The interoperability proposals regulate in Articles 20-22 only additional situations when authorities may access the repository.

The following section covers the main fundamental rights issues relating to the proposed Common Identity Repository, focusing in particular to the specific situations envisaged in Articles 20-22.

Using the repository to improve data accuracy

Article 17 (1) explains that the Common Identity Repository is created for three different purposes:

- correct identification of persons registered;
- supporting the functioning of the Multiple-Identity Detector (see Section 6);
- supporting access to the IT systems by law enforcement authorities.

The potential of the Common Identity Repository to improve data accuracy – a major flaw of the currently existing systems – is not mentioned in this context. Neither do Recitals 20-21 or Recitals 23-24 point to a possible benefit of the Common Identity Repository to improve data accuracy. Such a reference would, however, be useful to encourage Member States to maximise the use of the Common Identity Repository to correct inaccurate information in the identity data listed in Article 18 (1).

FRA opinion 9

FRA highlighted in its 2017 report on interoperability that low quality data could potentially magnify the negative effects on the individual. Through interoperability, the authorities have increased possibilities to become aware of inaccuracies and to address these.

The EU legislator could mention expressly the value of the Common Identity Repository to improve data accuracy in one of the relevant Recitals, taking inspiration from the wording included in Article 2 (2) (c) of the proposals.

Minimising identity data processed

Article 18 (1) lists the data to be included in the Common Identity Repository. As illustrated in Annex 1, the list of data is broader than the identity data defined in Article 4 (9) of the proposals. A careful review of each data item included in the Common Identity Repository is needed to see if the list included in Article 18 fulfils the objective declared in Recital 21,

[37] European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final, 12 December 2017, Explanatory memorandum, p. 7.

according to which only personal data strictly necessary to perform identity checks should be stored in the Common Identity Repository.

Such a review should also take into account the impact of each data item on the operation of the Multiple-Identity Detector, as well as on the possibility for the person concerned to prove his or her identity in case of doubts.

In FRA's view, most of the data included in proposed Article 18 (1) appear to be relevant to establish the identity file. However, the necessity of including the first name of the parents is questionable – see reference to Article 15 (2) (a) of the ETIAS Regulation in Article 18 (1) (c). First, ETIAS is the only system that records such information. The other IT systems do not have the names of the parents, apparently because it was not deemed necessary to process this data. Second, the names of the parents included in ETIAS are self-declared and not verified; thus, possible risks of misinterpretation cannot be excluded. These names are, therefore, more likely to contain mistakes, compared with identity data that are entered into a system by an officer who is bound by data accuracy obligations.

According to Recital 21 of the proposals, the Common Identity Repository should store only personal data that are "strictly necessary to perform an accurate identity check". As such, data are only collected for ETIAS and therefore cannot be compared across IT systems; storing the name(s) of a person's parent(s) does not appear to be necessary to perform an accurate identity check. For these reasons, FRA believes that the reference to Article 15 (2) (a) of the ETIAS Regulation in Article 18 (1) (c) does not comply with the principle of data minimisation, spelt out in Article 5 (1) (c) of the GDPR and Article 4 (1) (c) of the Police Directive, as well as Article 5 (c) of Convention 108.

FRA opinion 10

Most of the data included in proposed Article 18 (1) appear to be relevant to establish the identity file. However, the necessity of including the first name of the parents is not evident – see reference to Article 15 (2) (a) of the ETIAS Regulation in Article 18 (1) (c).

The EU legislator should amend the reference to Article 15 (2) (a) of the ETIAS Regulation in Article 18 (1) (c) of the proposals. Such reference should read "[the data referred to in Article 15 (2) (a) to (e) of the ETIAS Regulation, except the first name(s) of the parents of the applicant]".

Better clarifying access rights when using CIR to consult individual systems

According to Article 18 (2) of the proposals, the Common Identity Repository will include a reference to the information systems to which the data belongs.

FRA understands that depending on the situation, a user querying the Common Identity Repository will be authorised to see a different amount of information.

Articles 20 – 22 set out the special access rules for law enforcement to the Common Identity Repository, as well as in case of multiple identities. Leaving these aside, FRA understands that an officer searching the Common Identity Repository to access one of the underlying IT systems will only be able to see the components of the individual identity file that originate from IT systems which the officer is authorised to access, according to her or his user profile for the European Search Portal.

This solution seems to be supported by the last sentence of Recital 23, which refers to "duly authorised" officers, and by the tagging of data described in Recital 26. However, the proposals are not explicit on how access to the Common Identity Repository is regulated in case it is used as a vehicle to consult an individual IT system. In this regard, the wording of the proposals is unclear.

Example

Data on a person are stored in three different systems: A + B + C. An officer accessing the Common Identity Repository who is authorised to see only A + B will only see the identity data on the person which originate from A + B and nothing more.

FRA opinion 11

FRA understands that, when launching a query through the European Search Portal to consult an individual IT system, access to the identity data stored in the Common Identity Repository is subject to the rules set forth in the instruments regulating the individual systems. Nevertheless, in the absence of a reminder as to what data the user is entitled to see, the proposed articles concerning the repository could be interpreted in a way that is not compatible with Article 8 of the Charter.

The EU legislator should clarify in Article 18 – for example by adding a new paragraph after paragraph two – that an officer accessing the Common Identity Repository should only be able to see those components of the identity file stored in the repository which originate from IT systems he or she is authorised to access, indicating the legal provisions relating to the specific situations where the regulation provides otherwise.

Ensuring foreseeability and purpose limitation – access to the repository by the police for identification

Article 20 introduces the possibility for Member States to allow their police authorities to access the Common Identity Repository to identify people. The establishment of the correct identity is not an objective of interoperability – it is not listed in Article (2) (1) – but a tool to achieve this objective. This provision is vague and bears significant risks of violating the Charter during its implementation.

Defining a precise purpose at EU level

Article 20 (2) suggests that the police can consult the Common Identity Repository for two different objectives: to prevent or combat irregular migration as set out in Article 2 (1) (b) of the proposals as well as for internal security purposes as described in Article 2 (1) (c). The wording in Article 2 (1) (c) corresponds to the first part of Article 1 of the proposed SIS Regulation for police and judicial cooperation.

Article 20 does not precisely define at EU level when such identify checks are allowed. Article 20 (2) delegates the task of defining the precise purposes, competent authorities, procedures, conditions and criteria to Member States who wish to make use of this provision, in their national legislation. This provides Member States a degree of discretion that is not compatible with the requirement of the *Digital Rights Ireland* ruling; the ruling stipulates that EU law interfering with the fundamental rights enshrined in Articles 7 and 8 of the Charter should lay down clear and precise rules governing the extent of the interference.[38] The CJEU's

[38] CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 65. When examining the concept of necessity of data processing in *Huber*, the CJEU also clarified that the level of protection of the individual's rights with regard to the processing of personal data must be equivalent in all Member States. See CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008, para. 52.

considerations concerning the Data Retention Directive are even more compelling for the EU legislator when adopting a regulation that, by definition, is not limited to the results to be achieved but is binding in its entirety and directly applicable in all Member States (Article 288 of the TFEU).

Provided there is a legal basis in national law, the proposed provision would potentially allow the police to check anyone they stop for public order or for suspicion related to any criminal offence to verify the identity of the person against identity data stored in any of the interoperable IT systems (although the officer would not be informed about which IT system contains data on the individual). In other words, law enforcement authorities will be authorised to use the IT systems to identify a person for any security-related objective, even if all IT systems except SIS limit their access to "serious crime and terrorism".

Establishing access conditions to avoid abuse

Presumably, Article 20 should cover situations where people are physically stopped during a police check. Due to the undefined purpose of identity checks the use of Article 20 also entails a severe risk of discriminatory profiling, based on presumed ethnic origin or nationality. This regardless of whether the checks are carried out for internal security or immigration law purposes. Under proposed Article 24 (2), a police officer would have to provide only limited justification on why he or she checked the identity of a person against the interoperable IT systems. There is no need to show any suspicion against the person. Therefore, this provision opens up the risks of targeting members of specific communities generally believed to be more likely to be in conflict with the law or in an irregular situation.

This risk would be mitigated by establishing conditions that would limit the use of Article 20 only to those situations where consulting EU-wide IT systems would be necessary and proportionate to the objectives pursued. For example, it would be excessive to query the Common Identity Repository in case a person who is stopped shows his or her genuine identity document.

In principle, access to the Common Identity Repository by law enforcement authorities for internal security purposes should be limited to the situations regulated in Article 22. Article 20 opens the way for Member States to circumvent – at least partly – the stricter rules regulating law enforcement authorities' access to the IT systems as set in Article 22 (1). Although not revealing in which IT system data about a person are stored, the officer would know that at least one of the systems contains data on the individual. At least in some cases, depending on the circumstances, the police would be able to deduce which of the IT systems is likely to contain data on the individual and proceed directly to request full access to that data pursuant to proposed Article 22 (4). With high probability, the officer can often deduce where the data are stored based on the nationality, which reveals if the person comes from a country from which many asylum seekers originate, a country under visa obligation from which Europe receives many tourists or one that is visa free. For example, if biometric data on citizens of Afghanistan, Iraq and Syria have been stored, such data are far more likely to be stored in Eurodac and not in other systems. Similarly, biometric data on citizens of China or India, with a high probability, have been stored in VIS. By launching a query based on Article 20, police could thus circumvent the restrictions for law enforcement authorities to consult the Common Identity Repository listed in Article 22 (1). The strict access rules would thus only apply when the police wishes to access the data stored in the individual IT systems as per proposed Article 22 (4), which remain subject to the conditions and procedures set in the individual instruments governing each IT system.

Ex post controls

An additional safeguard to avoid a possible discriminatory use of Article 20 is to strengthen *ex post* controls. This could be done by increasing the type of information which is logged on the basis of Article 24 (2) to enable oversight authorities to establish if Article 20 is used disproportionately in certain locations or against certain individuals, as well as by requiring Member States to report on how this provision is used (See Section 10).

In addition, the practical handbook for the implementation and management of the interoperability components referred to in Article 67 could include, in concrete terms, safeguards to ensure that the implementation of identity checks under Article 20 does not result in discriminatory profiling or disproportionately affect fundamental rights.

Limit negative consequences for persons based on false matches

The proposals enable Member States to query the Common Identity Repository with biometric data or, if this fails, with alphanumeric data in line with Article 20. Particularly in situations in which the third-country national is not carrying a document – which is likely to be the most common situation for using the legal basis in Article 20 to consult the Common Identity Repository – or the document showed appears forged or fraudulent, the risk is high to receive identity data relating to other persons with the same of similar names. Limiting Article 20 queries to biometric data and travel document data only would reduce the risk of false matches and their negative implications for the individual as well as the authorities.

FRA opinion 12

Without defining the precise purpose for accessing the Common Identity Repository at EU level and establishing conditions limiting access, Article 20 bears a serious risk of being incompatible with Article 8 of the Charter. Moreover, queries using name, date of birth, and/or other biographic data are likely to lead to a significant number of false matches, with negative consequences for both the individual as well as the authorities.

The EU legislator should amend Article 20 – as well as the corresponding Recital 29 – to meet the requirements of foreseeability. To that end, the precise purposes of identity checks allowing to query the Common Identity Repository must be clearly set at EU level.

In addition, to comply with necessity and proportionality requirements, the EU legislator should set clear conditions for accessing the Common Identity Repository under Article 20, such as limiting the use of the provision to "the absence of a credible document proving the identity of the person". Article 24 (2) should also log the location of access and logs should be designed in a way to establish if the same person is checked multiple times.

To reduce the negative consequences of false matches, Article 20 should be amended by enabling only biometric searches and searches with travel document data.

Dealing with possibly erroneous red links

Article 21 (2) refers to red links, which are intended to signal situations of identity fraud.

Multiple identities may have different reasons. Apart from multiple lawful identities which give rise to a white link, differences in the data stored on the same individual in the IT systems may result from data entry mistakes – clerical mistakes, technical deficiencies, translation and transcription errors, for example. These are mistakes often caused by heavy

workload, insufficient guidance and other reasons.[39] They do not originate in an intention to commit identity fraud.

FRA research shows that there is a tendency to assume that data inconsistencies in the IT systems result from identity fraud. In case of data inconsistencies, applicants for international protection were suspected of concealing their correct identity. The registration in the other Member State was typically seen as being 'correct', with little possibilities to make changes. Sometimes the use of different names may simply be a personal choice without any secondary intention. Weak systems for civil registry in many developing countries enable the use of multiple identities.[40]

Pursuant to Article 32 (1), the verifying authority must classify a link as red whenever there are inconsistencies between different identity data and the authority concludes that the linked data refer unlawfully to the same person. This may include cases where the linked data shares the same biometrics but also cases where there are no biometric data to compare and the link is the result of similar biographic data.

Article 21 (2) indicates that in case of a red link the access to the data relating to the link is "solely for the purposes of fighting identity fraud". This seems to exclude that the authority can use the access also to initiate a correction, if it considers that the red link is erroneous.

It is of utmost importance to include a mechanism to correct erroneous red links as soon as any authority discovers it. This would mitigate the negative consequences for mistakes in IT systems for which the concerned person had no fault and which resulted in a red link and thus in a suspicion of identity fraud. In this context, the EES does not only contain a duty of the data controller to rectify mistakes but also a provision in Article 35 (3) whereby another Member State who has evidence about mistakes has either a duty to correct it or, if not possible, a duty to clarify the matter with the data controller.

FRA opinion 13

Given the negative consequences of a red link for the individual, Member States should be obliged to take all reasonable measures to rectify a link that has been erroneously marked as red.

The EU legislator should reinforce the obligation to correct mistakes by including somewhere in the proposal a provision inspired by Article 35 (3) of the EES Regulation obliging a Member State other than the data controller who has evidence about an erroneous red link to rectify it. Such a provision would support the horizontal efforts to ensure data quality, which are visible throughout the proposals.

Querying the repository for law enforcement purposes

Access to personal data by law enforcement represents a limitation on the right to respect for private and family life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter). As such, it must comply with the principle of necessity and proportionality. Usefulness of a measure is not in itself sufficient to comply with these requirements. According to the CJEU, even where a measure pursues an objective of general interest, including a fundamental one such as the fight against organised crime and terrorism, it does not in itself mean that the measure would be considered necessary for the

[39] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 82, 96.

[40] *Ibid.*, pp. 84, 95.

purpose as required by Article 52 (1) of the Charter.[41] Based on these principles, FRA has repeatedly emphasised that facilitating access to multiple databases at the same time should not be at the expense of existing safeguards and the purpose limitation which is in place for accessing each database.[42]

Conditions for law enforcement access and their relevance to a hit/no hit approach

EES, Eurodac and VIS all permit access for law enforcement "designated authorities"; law enforcement access is also proposed for ETIAS. With certain variations, they all require that such access is:

a) necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;

b) necessary in a specific case (ruling out systematic comparisons);

c) information contained in the IT systems to which access is requested is considered to substantially contribute to the objective of addressing terrorist or other serious offences. EES, ETIAS and Eurodac specify that this is particularly the case when there is a suspicion that the person falls in a category covered by the database in question.

In addition, EES, ETIAS and Eurodac all require a prior consultation of other databases with more direct law enforcement relevance. The exact design of this "cascade system" differs. In case of EES, it requires (at least for unknown suspects, perpetrators or suspected victims) prior consultation of national fingerprint databases as well as the automated fingerprint identification systems (AFIS) of other Member States available through the so-called Prüm mechanism based on Decision 2008/615/JHA.[43] The proposed ETIAS envisages prior consultation of "all relevant national databases" (as it does not contain fingerprints), as well as Europol data.[44] In the case of Eurodac, conceived as a system holding data of persons seeking international protection which are particularly sensitive, the requirements are most stringent.[45]

Under Article 22 of the proposal, access to the IT systems for law enforcement purposes is essentially divided into two steps. First, a law enforcement authority searches the Common Identity Repository on a hit/no hit basis to find out if data on the person are stored in the IT systems except ECRIS-TCN. The query can be conducted with biometric, biographic or travel document data. In this case, the authority querying the system needs to comply with essentially the same conditions as those listed above under (a) and (b) but there is no prior verification by an independent authority who would oversee if these conditions are fulfilled. Second, if the law enforcement authority wishes to consult the data stored in the individual IT systems, it will have to request access respecting the conditions and procedures laid down in the individual instruments regulating these.

In this manner, the proposed hit/no-hit system would simplify law enforcement access to the EU databases in two ways, by:

- removing the cascade system;

---

41 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 51.

42 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, p. 42; FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017, see for example Chapter 1 and 2.

43 EES Regulation, Art. 32 (2).

44 ETIAS proposal, Art. 45 (1) (d).

45 Eurodac Regulation Art. 20 (1); Eurodac proposal, Art. 21 (1).

- providing Member States' law enforcement authorities and Europol with information, without any verification requirements, in which EU databases the data relating to a specific person can be found.

One of the arguments for changing access conditions under the individual systems, in particular replacing the cascade system with a hit/no-hit query to the Common Identity Repository, is that such access conditions are considered unsuitable in practice. According to the European Commission, the challenges faced by the use of multiple identities justify consulting all systems to "determine the (possibly multiple and possibly differing) identity/identities of a person".[46] It should be noted, however, that contributing to fighting identity fraud is listed in Article 2 (2) (b) as one of the tools of interoperability and not one of its objectives. The objective of law enforcement access to EU databases is to combat terrorism and other serious crime. In the interoperability context, this corresponds to "contributing to a high level of security within the area of freedom, security and justice of the Union" (Article (2) (1) (c)). In this sense, law enforcement's access to the Common Identity Repository to ascertain which systems store data on a person is justified only to the extent that is necessary to achieve the objective of combating terrorism and other serious crime.

Multiple identities may be commonly used by persons involved in terrorism and other forms of serious crime, and access of Member States' law enforcement authorities and Europol to the Common Identity Repository can aid in detecting such cases. However, as shown in the subsection 'Dealing with possibly erroneous red links', cases of alleged multiple identity (or simply a false match with one of the databases) can exist for a variety of other reasons. This can lead to persons being flagged for law enforcement interest despite having no relationship to criminal activities. The fact that law enforcement authorities can conduct queries in the Common Identity Repository based on biometrics as well as on biographic and travel document data considerably increases the risk of a false match. It can therefore be questioned whether the hit/no-hit functionality, especially if used more often due to lack of a requirement of a prior verification of access conditions, is going to fulfil the intended objective of reliably establishing in which system the data on a specific person can be found. This is particularly valid when queries are launched without using biometrics.

Reducing law enforcement authorities' access to the Common Identity Repository to verify if identity data are contained in one of the IT systems cannot in itself justify the significant reduction of oversight and the removal of safeguards. Such safeguards need to ensure that those databases with more direct law enforcement relevance are consulted as well, in line with the principle of proportionality and purpose limitation.

Oversight by national verifying authorities

Under each of the IT systems national verifying authorities (central access points), which process the requests for comparisons, assess compliance with the access conditions. These authorities may, in practice, be part of the same organisational structure as the designated authorities submitting these requests, but they need to act independently and be separate from the operating units.

The hit/no-hit mechanism against the Common Identity Repository mirrors the conditions for access that are presently verified by the central access points prior to fully accessing the individual EU systems. According to Article 22 (1), the designated authorities may only consult/query the Common Identity Repository for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case to

[46] European Commission (2017), *Impact Assessment*, SWD(2017) 473 final, Strasbourg, 12 December 2017, p. 25.

obtain information on whether data on a specific person are present in one of the systems. This essentially corresponds to two of the three elements verified by the national contact point under the EES, Eurodac, VIS and future ETIAS regulations. The third element, evidence or reasonable grounds to consider that the consultation of the system will contribute to the objective, relies primarily on the suspicion that the person falls under the category of persons covered by the system, such as asylum seekers in Eurodac or visa-free travellers in ETIAS. This third condition is not present under the hit/no-hit system, which leads to a risk that queries of the Common Identity Repository would be conducted in any terrorism or serious crime investigations, regardless whether it is likely that the person can be found in any of the systems, or indeed is a third-country national at all.

Under the proposed interoperability regulations, the central access point is not required to verify compliance with the conditions for utilising the hit/no hit mechanism in Article 22 (1). The designated authority assumes the tasks. The central access point only verifies the request for full access.

The conditions required for full access to the IT systems and the conditions that need to be fulfilled to query the Common Identity Repository are similar. Therefore, a central access point's conclusion that the conditions for full access are not met would in most cases mean that also the conditions for querying the Common Identity Repository were not present in the first place. The *ex post* verification of logs envisaged in Article 24 (4) is a step in the right direction, but it does not offer the possibility of prior or at least parallel review of the conditions.

Consequently, consideration should be given to integrating an independent mechanism that would allow to assess, even on a non-systematic basis, whether the necessary conditions are met for querying the Common Identity Repository under Article 22 (1). This should not pose an obstacle to consulting the Common Identity Repository in justified cases; it should, however, ensure that the repository is only consulted in cases defined in Article 22 (1). Such a system could be based, for example, on flagging the queries to the Common Identity Repository which would be visible in real-time to the central access point or to the national supervisory authority, notably the national Data Protection Authority. Provided the authority is given the necessary resources, it would then have the opportunity to review the query and take appropriate action in case it would consider that the conditions of Article 22 (1) have not been not met.

Removing the cascade system

According to the European Commission, the cascade mechanism for accessing Eurodac and the future EES that requires first a 'Prüm' check through the crime databases of other Member States represents the main obstacle for law enforcement access to these databases. The need to submit a reasoned request to access each system in the cascade is described as leading to considerable administrative burden, resulting in delays and unnecessarily increasing the data flow.[47]

Instead of following the cascade system, the proposed regulations in Article 22 therefore allow national law enforcement authorities and Europol to consult the Common Identity Repository to ascertain which of the information systems contain matching data.

The concrete impact of this new approach on the law enforcement access modalities can be observed in the proposed modification to the EES Regulation which is contained in Article 55b of the interoperability proposal concerning the fields of borders and visas. The current provision of the EES Regulation requiring a prior search in national databases and, in

[47] European Commission (2017), *Impact Assessment*, SWD(2017) 473 final, Strasbourg, 12 December 2017, p. 25.

case of searches with fingerprints, of other Member States criminal databases (Article 32 (2)) is proposed to be replaced with a reference to a prior query to the Common Identity Repository, according to Article 22 of the interoperability proposal. A verification of the access conditions will only be undertaken by the central access point when a request for full access to EES is made.

A similar modification can be expected to be proposed in relation to the proposed ETIAS and Eurodac regulations.[48]

The existing conditions for law enforcement access to migration databases have been designed to reflect the ancillary nature of such access, which in the case of Eurodac and VIS was only added at a later stage, and to limit undue impact on individuals. As highlighted in the FRA Opinion on Eurodac, EU databases contain an increasingly comprehensive set of data on third-country nationals that is not available to Member States' law enforcement agencies and Europol for own nationals. This is particularly the case for biometric data – although databases storing biometric data at national level exist, they are usually limited to the storage of data of persons convicted or at least suspected of a crime, which offers a logical connection between the nature of the data and law enforcement.

Such a logical link is not clearly given in the case of law enforcement access to Eurodac, VIS or the future EES and ETIAS. The lack of an even indirect or remote connection between communication data retained and the purpose of their retention – serious crime – was among the arguments used by CJEU in the *Digital Rights Ireland* case to conclude that the Data Retention Directive was not in line with the Charter.[49] Although the data in EU databases are primarily collected for a different purpose, the ancillary law enforcement objective necessarily implies the need to take into account the principles outlined in the CJEU jurisprudence. The existing robust set of safeguards are of particular importance in Eurodac, given that a significant share of persons included in the database are applicants for international protection and persons granted international protection. Given the ongoing legislative procedure that aims to, among other modifications, include additional alphanumeric data in the system and therefore expand the amount of data potentially available to law enforcement, a parallel reduction in safeguards is difficult to justify.[50]

Besides ensuring adherence to the principle of purpose limitation, the different forms of the cascade system also serve to reflect the type of data contained in the individual EU systems, particularly as regards their sensitivity based on the categories of persons contained therein. Replacing the cascade system with a streamlined mechanism, such as the proposed hit/no-hit check against the Common Identity Repository means that data of all persons are considered equally sensitive and that data of persons in a vulnerable situation (such as that of persons seeking international protection) would not require enhanced safeguards.

Finally, the argument that prior consultation of other databases leads to delays and administrative burden is also not fully applicable. Firstly, it does not apply to national police databases which can be queried with a very short response time in all Member States. There

---

[48] See p. 11 of the proposed interoperability regulation: 'The other listed instruments (Regulations on ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) are currently under negotiation in the European Parliament and Council. For these instruments, it is therefore not possible to set out the necessary amendments at this stage. The Commission will present such amendments for each of these instruments within two weeks of a political agreement on the respective draft Regulations being reached.'

[49] CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, paras 58-59. See also CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 110.

[50] FRA (2016), *The impact of the proposal for a revised Eurodac Regulation on fundamental rights*, FRA Opinion [Eurodac], 06/2016, Vienna,, p. 41.

is, therefore, no substantial reason to waive the requirement of a prior check of the national databases. Secondly, the validity of this argument depends to a significant extent on the organisational setup of the mechanisms for the consultation of the individual systems at the Member State level. In case of Prüm cooperation, this applies to both the requesting and requested Member State, including the response capacity of their national AFIS. The reasons why Prüm cooperation is used to a different degree, and with different effectiveness and added value, by individual Member States, and the impact this has on addressing terrorism and other forms of serious crime, would deserve a detailed analysis. By querying the criminal databases of other Member States, the Prüm framework allows for the most comprehensive access to information that is already linked to criminal activities, suspects and perpetrators, i.e. information that can be considered to be of utmost relevance for ensuring a high level of security in Europe, one of the key objectives of interoperability. Streamlining of law enforcement access to EU databases should therefore not waive the requirement of consulting, at least in parallel, the AFIS of other Member States.

Removing the obligation to consult national police databases and automated fingerprint identification systems of other Member States (in case of fingerprint comparisons) would mean resigning on the primary dedicated law enforcement tools that offers, when it is used to its full potential, the highest likelihood of detecting information relevant to addressing terrorism and other forms of serious crime.

Logging

Querying of the Common Identity Repository by law enforcement authorities under the hit/no-hit mechanism constitutes in itself access to (albeit a limited amount of) personal data. As such, it represents a data processing operation and should be logged in order to allow for monitoring by the competent supervisory authority. Such *ex post* safeguards become of particular importance in case *ex ante* safeguards are reduced, although they play a different role and cannot fully replace them.

According to Article 24 of the interoperability proposals, eu-LISA must keep logs of all data processing operations within the Common Identity Repository. Paragraph 4 lists the information to be logged for queries conducted according to Article 22. This provision could be more specific to ensure that the logged data allows effective verification of the condition. For example, the item "national file reference" does not sufficiently clearly state that the query needs to be linked to an existing/ongoing investigation. Recital 32 is more explicit in this regard, clarifying that this refers to the "national file of the investigation or case, therefore indicating that such query was launched for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences".

FRA opinion 14

Access by Member States' law enforcement authorities and Europol to EU databases is permitted for the purpose of prevention, detection or investigation of terrorist or other serious criminal offences. Detection of multiple identities is one of the tools to achieving this objective but not a goal in itself. Therefore, it cannot in itself justify consulting the Common Identity Repository without any verification mechanism, and the removal of the cascade system which seeks to ensure that databases with more direct law enforcement relevance are consulted in the first place, in line with the principle of proportionality and purpose limitation.

Even if under Article 22 (1) the access by law enforcement is limited to verify if identity data on an individual are contained in one of the IT systems, this cannot in itself excuse the significant reduction of safeguards. A query in the Common Identity Repository already

reveals a certain amount of personal data and should not be based on an autonomous decision of the designated authority without any form of verification by an authority acting in an independent capacity.

Removing the obligation to consult national police databases and automated fingerprint identification systems of other Member States (in case of fingerprint comparisons) would mean resigning on the primary dedicated law enforcement tools that offers, when it is used to its full potential, the highest likelihood of detecting information relevant to addressing terrorism and other forms of serious crime.

Therefore, the EU legislator should:

- ***provide in Article 22 for a verification of queries to the Common Identity Repository by an authority acting in an independent capacity, such as the national central access point or, preferably, the national supervisory authority. Recital 33 of the proposals and, where necessary, the provisions concerning individual legal instruments in Articles 55b and 55e of the proposal in the field of borders and visas should be amended accordingly;***
- ***maintain in the legal instruments governing the individual EU systems as far as possible the cascade system and require, as a minimum, a prior check in national databases before querying the Common Identity Repository; Recital 34 of the proposals and Article 55b of the proposal in the field of borders and visas should be amended accordingly;***
- ***identify a solution for conducting a Prüm check before requesting full access to the information stored in the individual IT systems which does not unreasonably delay the consultation; Recital 34 of the proposal and Article 55b of the proposal in the field of borders and visas should be amended accordingly;***
- ***amend Article 24 (4) (a) replacing the current wording "the national file reference" with "the reference to the national investigation or case".***

6. Multiple-Identity Detector (MID)

The Multiple-Identity Detector is a tool to check whether a person is included in several IT systems. Such a check is performed any time when data are created or updated in any of the IT systems. It stores links between identities contained in different IT systems which are believed to belong to the same person. These links are classified as:

- white – in the case of clear identity (same or similar data referring clearly to the same person);
- yellow – in the case of unclear identity;
- green – in the cases of confused identity (two different persons with similar data);
- red – in the case of identity fraud.

The Multiple-Identity Detector intends to ensure the correct identification of an individual through **an automated as well as manual verification process**. The automated verification will work with algorithms. In case of multiple identities, the automated verification clarifies whether a link is white – namely sharing the same or similar identity – or yellow. Yellow links are subject to a manual verification after which they will be categorised as white, green or red.

This section describes the fundamental rights issues FRA noted in relation to the proposed Multiple-Identity Detector.

Mitigating unfavourable treatment of persons with multiple or confused identities

Article 5 of the two proposals establishes that the processing of personal data for interoperability purposes must not result in discrimination. In addition, according to Recital 37, the Multiple-Identity Detector should contain safeguards against discrimination or unfavourable decisions for persons with "multiple lawful identities". However, there is no express safeguard included in Chapter V of the proposals on the Multiple Identity Detector. The way to deal with these situations is delegated to the European Commission, which Article 28 (5) tasks to draw up implementing acts.

The envisaged automated mechanism of the Multiple-Identity Detector would link identity data in different information systems and classify these links based on whether the data are identical or similar. This can affect different categories of persons in different ways. Persons with multiple lawful identities stored in IT systems are likely to be stopped more often, for example, when they enter or exit the EU, particularly if biometrics of the person have not been stored. They would risk missing flights or other important commitments. Without sufficient safeguards protecting categories of people particularly affected, such different impacts will amount to discrimination.

One of the discriminatory criteria, as mentioned in Section 1, may be sex. Depending on how the algorithm filtering white links is designed, the change of a surname, combined possibly with a change in passport details (following the renewal of a lost passport, for example), could result in a yellow link triggering the need for a manual verification. While there may be a variety of reasons for the change of a name, the most common one is due to a marriage. The vast majority of persons affected will be women. Such discriminatory effects could be reduced if the Multiple-Identity Detector took into account also names at birth.

A second category of persons who are likely to be stopped for manual verification more often than others are people with dual nationality who travel on different passports.

Another category of persons are those with very common names – e.g. Mr Mohammed or Ms Lee – whose identity may be erroneously confused with the identity of another person, particularly in the absence of biometric identity data. If the verification procedure functions optimally, the green links would result in that persons with similar names would not be stopped, as this link would not be visible to the officer. The officer would not be aware of the existence of the green link, as the reply from the queried information system would indicate only the data of the person concerned, without triggering a hit against the data that are subject to the green link (Article 31 (2)).

Article 29 (4) as well as Recitals 58 and 59 of the proposal in the field of borders and visa clarify that where a yellow link is obtained, the border authority shall carry out additional verifications as part of a second-line check. This is accompanied by proposed amendments to Article 8 of the Schengen Borders Code (Regulation (EU) 2016/399) which would require border guards – at any check on entry or exit – to refer an individual to a second line check in case of a yellow or red link.

For the concerned person, a referral to a second line check entails that more time will be necessary for the border check with a risk of missing a flight or otherwise unduly delaying the onward journey. Given the significant negative consequences for the individual, a duty to refer a person systematically to second line checks, particularly in case of yellow links, is not proportionate. Border guards should maintain the flexibility to decide if a second line check is proportionate in light of the obligation deriving from Article 7 (1) of the Schengen Borders Code which requires that any measures taken "be proportionate to the objectives pursued by such measures". The border guard could inform the traveller to contact the relevant authority to resolve the yellow link subsequently.

FRA opinion 15

The proposals do not contain concrete safeguards against discrimination or unfavourable decisions for persons with "multiple lawful identities", delegating this to the European Commission who is tasked by Article 28 (5) to draw up implementing acts. At the same time the proposed duty to refer all persons with a yellow or red link undergoing border control to a second line check contradicts the proportionality safeguard in Article 7 (1) of the Schengen Borders Code.

To reduce possible disproportionate negative effects on women and other categories of persons with multiple lawful identities, the EU legislator should add an explicit reference at the end of the first sentence of Article 28 (5) underlining that such implementing acts should be designed in a manner that protects persons with multiple lawful identities against discrimination.

The EU legislator should amend Article 55 a of the proposed Interoperability Regulation on borders and visas, as well as Article 29 (4), Recitals 58 and Recital 59 of the respective proposal by removing the duty to refer any person with a yellow or red link to a second line check, in light of the obligation deriving from Article 7 (1) of the Schengen Borders Code.

Preventing negative effects of inaccurate ETIAS data

The Multiple-Identity Detector covers also ETIAS, as described in Article 25. The information stored in ETIAS is self-declared and not verified. It is, therefore, potentially less reliable than information entered into an IT system by a Member State that is bound by the duty to ensure data accuracy. It is also possible to imagine cases where the ETIAS file is fraudulently

completed – for example by a husband who enters erroneous data on his wife to prevent her from travelling.

An automated search for multiple identities will be launched when an individual file is created or updated in the EES, VIS, ETIAS, Eurodac, ECRIS-TCN or an alert is entered or updated in SIS, according to Article 27 (1). Pursuant to Article 27 (2), the automated search is carried out using the shared Biometric Matching Service for biometric data stored in the Common Identity Repository and SIS. ETIAS is the only IT system that will not include biometric data. Therefore, for ETIAS the automated search will use alphanumeric data contained in the Common Identity Repository (see Article 27 (3)). Inaccuracies in the ETIAS file may result in an unclear link with identity data stored in another IT system triggering a yellow link and a compulsory second line check when entering the EU. In the absence of biometric data to help verify the link, doubts about the link may remain also after the responsible authority has tried to carry out the verification. As a result, the link could be maintained as yellow for a considerable time, entailing problems for the person at least until he or she crosses the border, when the yellow link should be subject to manual verification.

FRA opinion 16

Automated searches for multiple identities across the IT systems are less reliable for ETIAS, because it does not contain biometric data. Depending on the sophistication of the algorithm used for the automated verification, this may result in an increased number of yellow links of persons whose data are also processed in ETIAS.

To reduce the negative impact of inaccurate identity information stored in ETIAS, the system should flag to the user when a yellow link is the result of inconsistencies with the identity data contained in ETIAS. The Handbook envisaged in Article 67 should provide guidance to Member States on how to deal with such situations without creating a disproportionate burden on those persons, who, without any intention to deceive the authorities, have entered inaccurate or ambiguous data in ETIAS.

Clarifying access rights and purpose limitation

In the two following situations, the authorities having access to at least one of the IT systems are authorised to see all identity data stored on the individual in the Common Identity Repository (leaving aside special rules concerning SIS data in Article 29 (2)), including a reference to the information system the data originates from:

- to verify different identities manually – Article 21 (1), Article 26, Article 29 (3); and
- when searches are carried out in case of a red link – Articles 21 (2) and 26 (2).

The proposed Interoperability Regulations will thus give an officer the authorisation to see personal data stored in IT systems to which they would otherwise have no access. In its 2017 report on interoperability, FRA highlighted that the simple knowledge of data being stored on an individual in a particular IT system may influence the conduct of an officer, even if the officer does not have access to the underlying information. Although access would be limited to identity details and only to the IT system where the data originate, it provides access to information that goes beyond what the officer is entitled to see under the instruments regulating the individual IT systems. It therefore may create bias in the decision-making concerning the person.

In practice, such risks are highest with ECRIS-TCN, Interpol and Europol data. Whereas the proposals limit the access to Interpol and Europol data – as neither of the two are used to create the identity file in the Common Identity Repository, the situation is different with ECRIS-TCN.

The following example illustrates the risk this can create: a person who was convicted of a crime but who was not issued an entry ban or his/her entry ban has expired travels to the EU and is checked at the border crossing point. The border guards query the IT systems and see that identity data on the same person are stored also in ECRIS-TCN. The individual will in most cases be referred to a second line check, either because of a yellow or red link or because he/she may be considered to pose a threat to public policy or internal security as per Article 6 (1) (e) of the Schengen Borders Code. During the second line check, the past ECRIS-TCN entry will likely weigh against allowing the person entry into the EU. Individuals with past criminal records will thus continue to face negative consequences for what they did in the past, long after their sentence have come to an end.

Given the different national regulations of criminal records registers, ECRIS-TCN will include offences of varied severity, from serious crimes to misdemeanours.[51]

In practice, the Multiple-Identity Detector results in circumventing access rights to ECRIS-TCN, essentially allowing all authorities who have access to at least one IT system to know if a person has a past criminal record or not. In FRA's view, such an approach would not be compatible with the principle of purpose limitation set in Article 8 of the Charter.

Such extension of access rights to information collected by ECRIS-TCN should be subject to a detailed necessity and proportionality assessment to be carried out in the context of the adoption of the ECRIS-TCN Regulation and should not occur by the back door of interoperability.

According to the ECRIS-TCN proposal, queries in the system are to be conducted by the competent central authority of a Member State, in order to establish which Member State(s) holds criminal record information about a person. Purposes for which the system may be queried are nevertheless not strictly defined at the EU level. Only the use of ECRIS-TCN for criminal proceedings is defined at the EU level. Other purposes can be established in national law. This means that there is a potential for a high degree of divergence among Member States in querying the system. Through interoperability, authorities which would not even be able to submit a request to the central authority to undertake a query under national law will gain access to identity information and implicitly gain knowledge that the person has a past criminal record.

A tension with the principle of purpose limitation also exists for the other IT systems which an authority is normally not authorised to access but where it would become aware of data entries on an individual through Article 21 (1), Article 26, and Article 29 (3) of the proposed Interoperability Regulations. This would, for example, be the case when visa authorities are informed that identity data are stored in Eurodac or ETIAS or when the determining authority under the Asylum Procedures Directive sees that an applicant has also a record in the EES.

FRA opinion 17

In case of a yellow or red link, the proposed Interoperability Regulations will give an officer the authorisation to see personal data included in the identity file, stored in IT systems and to which they would otherwise have no access. In case of ECRIS-TCN this would allow a large number of authorities to see if an individual has a past criminal record. This does not appear compatible with the principle of purpose limitation in Article 8 of the Charter.

The EU legislator should delete Article 18 (1) (e) thus excluding ECRIS-TCN data from the Common Identity Repository.

[51] ECRIS-TCN proposal, Art. 2, Art. 3 (1) (a) and (c).

Improving manual verification of multiple identities – data quality

The proposed Interoperability Regulation establishes a two-step mechanism to verify the identity of a person. First, an algorithm will filter out entries with the same or similar identities and flag all other cases of multiple identities as "yellow". Second, an officer will verify manually all yellow links and determine if the different entries correspond to the same person (white link), to two different persons who have been confused (green link) or if it is a case of identity fraud (red link).

In the absence of sufficient evidence to assess the link, the officer will keep the link yellow. This may occur, for example, when the verifying authority finds it necessary to involve other authorities to seek further guidance. In this case, the person will be subject to further verification, when he/she applies for a visa or is checked at a border crossing point until the yellow link is resolved.

According to Recital 40, the national authority or EU body that recorded the data in the respective EU information system should confirm or change the coding of the links. For this purpose, such authority will be authorised to access the data stored in the Common Identity Repository or SIS and in the Multiple-Identity Detector. Article 29 lists the national authorities responsible for manual verification.

FRA research has confirmed serious data quality issues in the IT systems which are currently operational[52] and which will become interoperable. It also shows that data tend to include more mistakes when collected in stressful situations. Increased workload and strain on the staff affect the recording of data.[53] EES data will usually be collected under time pressure at border checks and are expected to represent the largest data category in the Common Identity Repository.

According to FRA research, identify fraud is not the only reason for multiple identities. Such situations do often not originate in a deliberate intention to deceive the authorities. Still, in most cases it affects how the trustworthiness of the person is perceived.[54] Building on the findings of FRA's research, it is therefore not unlikely that whenever an officer cannot find immediate plausible explanations for the inconsistency in identity, there will be a tendency to create a red link, showing that it is a case of identity fraud. Such a risk is highest with those systems where the identity data are not taken from a document, but are the result of an interview with the person (as is often the case of data entered in Eurodac, where identification interviews may take place without interpretation and under difficult conditions and the data recorded is not cross-checked by the person concerned) or where the individuals themselves enter the data and may make mistakes (as could be the case in ETIAS).

Every officer who is authorised to create or update a record in one of the systems is also responsible for assessing the reasons behind multiple identities. This includes a very large number of officers across the EU, with different level of expertise and training. Even with detailed guidance, it is difficult to imagine how a consistent and fair approach across the EU could be achieved in determining if a link should be coded as white, green or red or if it should remain yellow. In practice, the situations will be so different that officers will likely have significant discretion in each specific case.

---

[52] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, Section 5.1.

[53] *Ibid.*, p. 84.

[54] *Ibid.*, p. 95.

Particularly at border crossing points, border guards can be expected to have to undertake a large amount of manual verifications based on yellow links. To meet the objective of ensuring a smooth flow of traffic and not to create long queues at borders and inconveniences, such as missed flights, officers will be under pressure to assess the type of link as quickly as possible. The number of trained staff and of dactylographic experts would have to be considerably increased. This measure will not only be needed in the border management context but also for visa, asylum and other procedures, highlighting even more the need of ensuring a consistent and fair approach in the verification.

Two measures could be taken to reduce the risk of mistakes in defining the type of links.

1) FRA research shows that data stored in IT systems are more accurate when the person concerned is given the opportunity to verify what is recorded on him or her. The data subject has the possibility to clarify contradictions when mistakes are discovered. In some EU Member States, at least in certain situations, the person has to read and verify the information being inserted.[55] Acknowledging the risk of mistakes and involving the person concerned in preventing this would therefore be important, both as a fundamental rights safeguard and to allow more effective classification of links.

   Articles 32 and 33 contain a duty to inform the person (subject to certain limitations and only in relation to red and white links) but not an obligation to give the opportunity to explain the reasons for the differences in the IT systems. Recital 42 contains such a due process approach suggesting that the assessment of the link should be done in the presence of the third-country national, where possible but is formulated in soft terms and not followed up in the operative part of the proposed regulations.

2) The risk for data subjects to be confronted with an erroneous link or with the negative consequence of a yellow link that is not cleared can be achieved through measures promoting a consistent and fair approach among all authorities in charge of verification. This could be achieved by designating at national level a central authority to support verification.

   The designation of such a national central authority would not only benefit the data subject but also complement other data quality measures contained in the proposals. Such a designated national authority could also become eu-LISA's counterpart at national level for improving the quality of identity data, coordinating the work undertaken at national level by the responsible authorities for each system to improve the quality of data in that system. It could support implementation of and compliance with standards developed by eu-LISA, and could provide training and other support on data quality matters at the national level.

FRA opinion18

The colour coding of a link between different identities significantly affect a person's fundamental rights, particularly if the link is assessed as "red", meaning that it is considered as a case of identity fraud or when a yellow link remains as such over a considerable period of time. Effective measures are needed to reduce this type of negative impact.

The EU legislator should include a horizontal provision, for example in Article 29, reflecting the statement in Recital 42 and thus requiring, whenever possible, the authority

[55] *Ibid.*, p. 85.

responsible for the manual verification to consider plausible arguments presented by the third-country national when deciding on the colour of the links.

The EU legislator should introduce a duty for Member States to designate a central verification authority at national level. Such an authority should include staff with fundamental rights expertise. This authority would have the task to provide guidance to the authorities in charge of the verification, monitor their work and develop best practices through cooperation in a network of other central verification authorities in other Member States. It could also support eu-LISA with the improvement of data quality.

Informing data subjects in case of a red link

While Section 8 deals with the right to information overall, this subsection analyses the provisions that regulate the duty to inform in case of a red link.

Articles 32 (4) and 33 (4) regulate the duty to inform the person in case of a red or white link. There is no corresponding provision in relation to green links, as the querying officer does not see the green link, thus no hit is created (Article 31 (2)). The duty to inform contained in Articles 32 (4) and 33 (4) is subject to the restrictions applying to SIS alerts. In case of red links, the duty to inform is also subject to restrictions "necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised." The restriction goes beyond the wording of the three SIS proposals, as it includes "public order". Given the broad possibilities to limit the duty to inform, possibilities for the third-country national to rebut a false assumption are excessively restricted.

The restrictions could also disproportionately affect the persons' right to an effective remedy, as protected under Article 47 of the Charter, in addition to being a disproportionate infringement of the rights to respect of private life and protection of personal data. As the CJEU has noted, in the context of security measures affecting the right to private life and the right to the protection of personal data, national law enforcement authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer capable of jeopardising the investigations undertaken by those authorities. The Court has held that notification is, in fact, necessary to enable the persons affected by these measures to exercise, inter alia, their right to a legal remedy guaranteed in Article 47 of the Charter.[56]

A further question is the possibility to claim compensation for damages in such a situation, an issue that is already very difficult with regard to existing IT systems, as FRA research shows.[57] This issue is dealt with in Section 9.

FRA opinion 19

Articles 32 (4) and 33 (4) regulate the duty to inform the person in case of a red or white link. They introduce restrictions that appear difficult to justify.

The EU legislator should strengthen the duty to inform by deleting public order from the list of grounds of restrictions in Articles 32 (4) and by ensuring that, in the case of red links, third-country nationals are still notified, as soon as such a notification is no longer capable of jeopardising on-going investigatory proceedings.

---

[56] CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, para. 121. See also, *mutatis mutandis*, CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, 7 May 2009, para. 52; CJEU, C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, para. 95.

[57] FRA (2018), Under watchful eyes: biometrics, EU IT systems and fundamental rights, Luxembourg, Publications Office, March 2018, Chapter 6.

7. Reporting and statistics

Article 39 of the proposals will establish a Central Repository for Reporting and Statistics. As explained in Recital 47, the Central Repository hosted by eu-LISA will be used to generate statistical data and analytical reports for policy, operational and data quality purposes.

Recital 47 explains that the repository will contain anonymised data from the underlying IT systems, the shared Biometric Matching Service, the Common Identity Repository and the Multiple-Identity Detector. The exact data categories which will be included in the Central Repository for Reporting and Statistics will be defined in the legal instruments regulating the underlying IT systems. For the EES, it covers the data listed in Article 63 (1) of the EES Regulation, namely: status information; nationality, sex, and year of birth; border crossing details; travel document information; number, nationality and entry border crossing point of over-stayers; information on revocation or extension of stay; the Member State issuing the visa; the number of persons exempt from giving fingerprints; as well as details on persons refused entry.

Reliable statistics are important to assess at regular intervals the proportionality of the different components of interoperability, as well as to provide data for an evidence-based approach in the implementation of border management and visa policies. However, there are also fundamental rights concerns.

First, according to Article 39 (2) the repository will only contain data which do not enable the identification of individuals. The anonymisation will be done automatically by eu-LISA (Article 39 (3)). According to Article 89 (1) of the GDPR, adequate technical and organisational safeguards need to be in place for the anonymisation to be achieved effectively. In this context, solutions must be applied which prevent also an indirect identification through the combination of different data elements. For example, in case of data subjects from small island states in the Pacific, even where the name and the passport number is removed from the repository, an individual may still be identified through a combination of nationality, sex and year of birth.

Second, the Central Repository for Reporting and Statistics will offer an unprecedented large pool of data, permitting the production of "customisable reports and statistics" for a broadly defined range of purposes. Furthermore, access to the data, according to Article 56, is quite broad. At the EU level, in addition to eu-LISA, the European Commission and Frontex have direct access to the repository. At a Member State level, it will be "duly authorised staff of the competent authorities".

The statistics and report which will be produced may be of considerable value for monitoring the functioning of the system, but also for the creation of targeted, evidence-based policies and risk analysis, including at the Member State level. If such policies and risk analysis are based on – even anonymised – data, such as nationality, sex and age, or the combination thereof (which Article 56 (2) and (3) seem to foresee), there is a clear need for safeguards to reduce the risk that personal bias may consciously or unconsciously lead to the production of reports suggesting operational actions which would result in discrimination of certain categories of persons.

One possibility to mitigate this risk is to oblige Member States to channel all requests for statistics and reporting through a single access point. Instead of giving access to the repository to the different national authorities who may wish to use it for their operational needs, these would have to request one designated authority to produce the statistics and reports they need. The interoperability handbook envisaged in Article 67 could provide guidance on how to carry out this task so as to ensure that reports do not directly or indirectly

suggest actions which would be incompatible with the prohibition of discrimination. In addition, the designated central authority could be obliged to produce regular reports on their operation and on the use of the repository. This would allow the European Commission to receive regular information from Member States on how the Central Repository for Reporting and Statistics is used, which could serve to assess the impact of this part of the interoperability proposals according to Article 68 (5).

FRA opinion 20

Article 39 aims at establishing a Central Repository for Reporting and Statistics, which will contain anonymised data on a very large number of persons. Even if data are anonymised through an automated system, there are still risks attached to creating such a repository, which call for safeguards.

The EU legislator should consider strengthening the provision in Article 39 (3) by requiring that the personal data be truly anonymised, i.e. made non-identified and non-identifiable, so as to avoid also the risk of indirect identification of individuals whose data are stored in the Central Repository for Reporting and Statistics. Additionally, Article 56 (2) (b) and Article 56 (3) (a) referring to "nationality, sex and year of birth of the persons" should be complemented with a safeguard noting that this should "not lead to identification of the person concerned".

To mitigate the risk of discrimination when producing reports on the basis of the Central Repository for Reporting and Statistics, the EU legislator should redesign Article 56 by requiring Member States to assign the responsibility to produce statistics and reports to a designated central point.

The possibility to receive customisable statistics on the use of the repository by eu-LISA could be extended to relevant EU agencies when needed to evaluate the impact on fundamental rights of the interoperability regulations.

8. Right to information

The provision of information is a transparency requirement under data protection law. It promotes respect for the dignity of the person, protected in Article 1 of the Charter, by enhancing the person's cooperation and thus reducing the risk of coercive measures, for example, to take fingerprints. This is important since individuals may perceive the taking of their biometrics as unpleasant.[58] The provision of information is also a precondition to effectively exercise one's right to access, correction and deletion of personal data.

In line with Recital 48, the GDPR and the Police Directive apply to the processing of personal data for interoperability purposes. Both legal instruments include provisions guaranteeing the right to information. Article 5 (1) of the GDPR requires that personal data are "processed lawfully, fairly and in a transparent manner in relation to the data subject". In line with Article 12 of the GDPR, controllers must take appropriate measures to inform third-country nationals about the relevant aspects of their personal data being processed in a transparent, intelligible and easily accessible form.[59] According to Articles 13 of the GDPR and the Police Directive, and Article 14 of the GDPR, the person concerned should receive, among others, the following information: the identity and the contact details of the controller; the purpose of the processing; the retention times; the right to request access to stored data and their erasure or rectification; as well as the right to lodge a complaint with a supervisory authority.

To improve the effectiveness of information provided and comply with the transparency requirements when processing personal data under the GDPR, the Article 29 Data Protection Working Party developed guidance for data controllers.[60]

This section analyses how the duty to inform is designed in the context of interoperability. It builds significantly on FRA's research findings which show the considerable practical challenges to inform persons in an effective manner in relation to the already existing IT systems.

Making the right to information more effective

Article 46 of the interoperability proposals includes the obligation of the authority collecting the data which are processed in the shared Biometric Matching System, the Common Identity Repository and the Multiple-Identity Detector to inform the data subjects, when collecting their data, about the processing of personal data for the purposes of interoperability. The duty to inform the person at the time their data are collected is an important safeguard, as reflected also in Article 13 of the GDPR. It helps to ensure an effective right to information, since authorities collecting the data are in (often direct) contact with the data subject and can, therefore, ensure that the information is provided in an appropriate manner, sensitive to the age, gender and background of the data subject and taking into account their needs.

The disrespect of the duty to inform may lead to decisions affecting a person based on unlawfully stored data.[61] If individuals do not receive enough information about their data stored, it is also difficult for them to exercise the right to access, correction and deletion.[62]

---

58 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 43.

59 See also Article 12 of the Police Directive which contains a similar wording.

60 Article 29 Data Protection Working Party (2017), WP29 Guidelines on transparency under Regulation 2016/679, WP 260.

61 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 29.

62 *Ibid.*, p. 29.

Content of the information

According to the proposals, such information includes identity and contact details of the respective data controllers, contact details of EDPS and the national supervisory authority and information on procedures for exercising their rights of access, correction and erasure. However, it does not expressly say, for example, that the person should be informed about the *different purposes* for which his or her personal data will be processed (including by law enforcement agencies), who the data recipients are, and for how long the data will be stored. The EU data protection *acquis* contains a duty to cover also these aspects.[63] In addition, pursuant to Article 77 of the GDPR and Article 52 of the Police Directive, the information provided should also cover the right to lodge a complaint with a supervisory authority.[64]

Although the duty to provide the comprehensive set of information as required by the EU data protection *acquis* applies fully to the data processed under the interoperability proposals, in light of the practical difficulties documented in its research,[65] FRA considers it extremely important to re-state some of these aspects in Article 46. This will help increase the awareness of what the duty to inform entails.

This is particularly the case for the purpose of processing, the recipients of the data and the retention time. FRA findings indicate that transparency about the purpose of data collection encourages the persons concerned to cooperate with the authorities. For example, asylum applicants and migrants in an irregular situation perceive EU Member States to be acting in a non-transparent manner if authorities provide no or only limited information on fingerprinting procedures. This affects their willingness to cooperate with them.[66]

How to provide information

Article 46 does not include any detailed provisions on the manner in which information should be provided to the data subject. The controllers are obliged to provide information in line with the relevant GDPR and Police Directive provisions, this is in a concise, intelligible and easily accessible form, using clear and plain language. Information must be provided pursuant to the GDPR also in a transparent form.[67]

According to the research conducted for FRA's report on biometrics, authorities that collect personal data of asylum and visa applicants, as well as of migrants in an irregular situation, and then store these data in IT systems find it challenging to provide information in an understandable manner. Rights holders are often not fully informed of all aspects of the data processing and have difficulties understanding the information they receive. This is particularly true when the information system at issue serves a number of purposes and processes.[68] The research confirmed past FRA findings, that persons lack awareness of data protection violations and available remedies.[69]

---

63 See for processing purposes: GDPR, Art. 13 (1) (c), Art. 14 (1) (c); Police Directive, Art. 13 (1) (c); for retention periods: GDPR, Art. 13 (2) (a), Art. 14 (2) (a); Police Directive, Art. 13 (2) (b) – in specific cases; for data recipients: GDPR, Art. 13 (1) (e), Art. 14 (1) (e); Police Directive, Art. 13 (2) (c) – in specific cases.

64 As included in GDPR, Art. 13 (2) (d), Art. 14 (2) (e); Police Directive, Art. 13 (1) (d).

65 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, Chapter 1.

66 *Ibid.*, pp. 9, 33-35.

67 GDPR, Art. 12 (1); Police Directive, Art. 12 (1).

68 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 9.

69 See: FRA (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office, May 2010; FRA (2012), *Access to justice*

Recital 38 of the GDPR requires special protection regarding the processing of personal data of children. Recital 58 and Article 12 of the GDPR as well as Recital 39 of the Police Directive include a reference on providing information to children in an appropriate manner. Also Eurodac contains a safeguard to provide information to children in an age-appropriate manner, which could be taken as an inspiration for the interoperability proposals.[70]

FRA opinion 21

With interoperability, ensuring the right to information will become increasingly challenging. Strengthening the duty to inform in Article 46 would help in addressing at least some of the practical difficulties that FRA research documented as obstacles for an effective provision of information.

The EU legislator should consider the following measures to strengthen the right to information included in Article 46 of the proposals:

- ***expressly require that the information provided should also cover the different purposes of the data processing, who the recipients of the data are and the retention time, as well as the right to lodge a complaint with the supervisory authority;***
- ***add explicit information on the fact that personal data may be accessed by law enforcement authorities, drawing upon Article 50 of the EES Regulation and Article 30 of the Eurodac proposal;***
- ***taking into account the target audience (i.e. third-country nationals), add an explicit provision on providing information in a language that the person understands or is reasonably expected to understand, drawing on Article 30 of the Eurodac proposal and Article 50 of the EES Regulation;***
- ***add an explicit reference to providing the information to children in an age-appropriate manner, drawing upon Article 30 (2) of the Eurodac proposal, as well as Recital 58 and Article 12 of the GDPR and Recital 39 of the Police Directive.***

Ensuring every category of persons is informed

Article 46 (2) lists situations in which persons whose data are recorded in ECRIS-TCN, EES, ETIAS, Eurodac and VIS must be informed, in line with Article 46 (1), about the processing of their data for interoperability purposes. Essentially, it provides for a duty to inform the person when a file "is created or updated" in the individual IT system. A file might, however, be created after the collection of data, as for example in the case of Eurodac, which includes a time limit of 72 hours to submit the data to the Central System. However, the most meaningful moment to inform the data subject is at the moment when their data are collected. This provision should not lead to delaying the duty to inform "at the time [...] data are collected" set out in Article 46 (1).

In addition, Article 46 (2) does not cover all categories of persons whose data are processed in one of the underlying IT systems. First, Article 46 (2) (d) excludes irregular migrants registered in Eurodac. Second, Article 46 (2) excludes persons whose data are or will be processed in the SIS Regulation (i.e. persons subject to an entry ban) and in the proposed SIS Regulation on return.[71] The right to information applies also to them, at least under

in cases of discrimination – Steps to further equality, Luxembourg, Publications Office, December 2012; FRA (2017), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update*, Luxembourg, Publications Office.

[70] Eurodac Regulation, Art. 29 (2); Eurodac Proposal, Art. 30 (2).

[71] SIS II Regulation, Art. 42 (1); SIS II borders proposal, Art. 48, SIS II return proposal, Art. 13.

certain conditions. In situations where the right to information arises under SIS, the persons concerned should be also informed that their data will be further processed for interoperability purposes.

FRA opinion 22

The right to information in the proposed regulations do not encompass all categories of persons whose data will be processed in one of the underlying IT systems which will be made interoperable. This oversight should be corrected.

The EU legislator should:

- ***include in Article 46 (2) (d) also a reference to Articles 13 and 14 in addition to Article 10 of the Eurodac Regulation to cover also the collection of personal data of third-country nationals or stateless persons in an irregular situation;***
- ***extend the duty to inform also to all individuals who are processed under SIS.***

9. Right of access, correction and deletion

Article 8 (2) of the Charter, as well as the GDPR, the Police Directive and Council of Europe Convention No. 108 guarantee the right to access, correction and deletion of collected personal data.[72] The right to access under Article 15 of the Police Directive may be restricted, provided the measure is necessary and proportionate for specific reasons. The specific legal instruments regulating the IT systems also mirror the right to access, correction and deletion,[73] with limitations applying in regard to SIS.[74]

EU IT systems contain a significant amount of inaccurate alphanumeric data. Evaluations by the European Commission, the European Data Protection Supervisor (EDPS) and the High Level Expert Group on information systems and interoperability have underlined problems with data accuracy in SIS[75] and VIS[76].[77] FRA's recent publication on EU IT systems and biometrics also confirms such problems: about half of the border guards and also diplomatic mission and consular staff who participated in FRA's small-scale survey (as part of its research on large-scale IT systems set up by the EU in the field of asylum and migration) indicated that they at least sometimes experience inaccurate, incorrect or not updated personal data in VIS or SIS.[78] Although rare, FRA field research did reveal individual incidents of Dublin transfers being carried out based on false biometric matches.[79]

National authorities and experts attach a high degree of credibility to biometric data, and processing such data is technically complex. This makes it difficult for persons concerned to rebut errors in IT systems, and even more difficult to prove that a biometric match was incorrectly generated.[80]

Interoperability offers new opportunities to correct inaccuracies. Both, the individual as well as the authorities have an interest in ensuring that the data stored are accurate. However, tackling the data quality issue in IT systems is difficult, requiring strong commitment by Member States' authorities and EU agencies to take all reasonable steps to eliminate mistakes in the systems. This section suggests ways to enhance in practice the possibilities a data subject has to get mistakes corrected.

---

72 GDPR, Art. 15-17; Police Directive, Art. 14 and 16; Council of Europe Convention No. 108, Art. 8.

73 See: Eurodac Regulation, Art. 29 (4) and (5); Eurodac proposal, Art. 31; EES Regulation, Art. 52; ETIAS proposal, Art. 54; ECRIS-TCN proposal, Art. 23; VIS Regulation, Art. 38; Interoperability proposals, Art. 47.

74 SIS II Regulation, Art. 41; SIS II Decision, Art. 58; SIS II police proposal, Art. 65; SIS II borders proposal, Art. 47; SIS II return proposal, Art. 13.

75 European Commission (2016), *Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66 (5) of Decision 2007/533/JHA*, COM(2016) 880 final, Brussels, 21 December 2016; European Commission (2016), SWD(2016) 450 final, Brussels, 21 December 2016.

76 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), Commission Staff Working Document, *Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation*, SWD(2016) 328 final, Brussels, 14 October 2016.

77 European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, OJ 2008 C 200/1, p. 2; High Level Expert group on Information Systems and Interoperability, Register of Commission Expert Groups.

78 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 82, 83. Available also in: FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017, pp. 30, 31.

79 *Ibid.*, p. 15.

80 *Ibid.*, p. 16.

Regulating access, correction and deletion of data stored in the Common Identity Repository

Article 47 of the interoperability proposals regulate the right to access, correction and erasure of data stored in the Multiple-Identity Detector. Under the proposed wording, this provision does not apply to mistakes contained in the identity data stored in the Common Identity Repository which derive from the underlying IT systems.

Under proposed Article 40 the controller of the data in the Common Identity Repository remains the Member State authority that is the controller of the data in Eurodac, VIS, the EES, ETIAS and ECRIS-TCN. This means several dozen authorities across the Member States.

In practice, an error in the Multiple-Identity Detector will typically be based on inaccurate or unlawfully stored data in the Common Identity Repository. Therefore, the correction of mistakes in the verification of the links between identities will frequently require also a correction of the data stored in the Common Identity Repository.

Moreover, in many cases the data subject will be made aware of inaccurate data when an authority queries the interoperable systems through the European Search Portal and get a yellow or red link as a response.

The proposed solution in Article 47, which addresses only mistakes resulting from operation of the Multiple-Identity Detector and not those included in the Common Identity Repository, appears inappropriate. It promotes a highly fragmented way to exercise the right to correction and deletion, which is deemed to remain ineffective.

FRA opinion 23

Existing IT systems contain a significant amount of mistakes in the accuracy of data. Such mistakes can have serious consequences for individuals, which risk to multiply with interoperability. The proposed regulations should therefore offer a better solution to help individuals to correct mistakes not only in relation to the Multiple-Identity Detector but also for the Common Identity Repository.

The EU legislator should therefore extend the scope of Article 47 on the right of access, correction and erasure of personal data to cover also the Common Identity Repository.

Making corrections of mistakes possible in practice

To exercise the right to access, correction and erasure, the person concerned needs to receive clear and unambiguous information on how to do it and procedures need to be as user-friendly as possible. Individuals often lack awareness and understanding of what needs to be done in case of mistakes in their personal data processed by the systems. The Supervisory Groups for SIS II and VIS also pointed to the same lack of awareness.[81]

Establishing an EU-wide request handling mechanism

The cumbersome nature of the process discourages affected people from initiating procedures. According to FRA research, administrative hurdles and language barriers, difficulties in understanding the procedures and few specialised lawyers are the main

[81] SIS II Supervision Coordination Group (SIS II SCG) (2014), *Report on the exercise of the rights of the data subject in the Schengen Information System (SIS)*, October 2014, p. 15; VIS Supervision Coordination Group (VIS SCG) (2016), *Report on access to the VIS and the exercise of data subjects' rights*, February 2016, p. 15.

reasons behind the low numbers of persons who try to exercise their right of access, correction or deletion of inaccurate data that is stored in existing systems.[82]

These difficulties may be exacerbated when IT systems are made interoperable, as an individual will have to find out which Member State to approach and within it, which authority is responsible for handling the request as well as what evidence he or she needs to provide to get data rectified. Although there will be a duty for any authority to forward a request to the competent Member State, this will necessarily lead to delays, with possible further negative consequences for the person concerned. This might be particularly the case since the shared Biometric Matching Service (Article 13 (2)) and the Common Identity Repository (Article 18 (2)) will include only a reference to the relevant system but not to the responsible Member State.

An EU-wide request handling mechanism to manage requests to access, correct and delete data as well as to provide data subjects with the information they need would help data subject to initiate a request and follow up on it. This could be achieved through the establishment of an EU web-portal managed by eu-LISA. The EU-wide request handling mechanism would not alter Member States' responsibilities to process the requests in line with applicable law. It would simply serve as a tool to overcome many of the practical obstacles preventing corrective actions FRA observed in practice.

In practice, an EU-wide request handling mechanism could consist of a web-portal where a person who wishes to request access, correction or deletion of data could obtain information (through Frequently Asked Questions and contact details of controllers and national supervisory authorities, for example) and lodge a request. The EU-wide request handling mechanism would forward the request to the responsible authority but also advise where the data subject could go for support (for example, in case there is a need to re-submit fingerprints). Through logging of the steps taken, the data subject would always know where his or her request is pending and follow up with the specific national authority if need be.

Handling of requests in an electronic format might be of a particular advantage in the context of interoperability, since the data subjects might often not be present in the respective Member State. FRA research showed that speedy replies to a request for access, correction or deletion might be prevented by administrative obstacles, such as acquisition of a legal address to which the requested information can be sent, especially if the data subject comes from a conflict area. Member States might, as it is the case in one EU Member State, restrict the possibility to dispatch a reply only to an address in the respective Member State.[83] Nevertheless, to take into account the specific situation of persons who do not have (adequate) internet access,[84] there should also be alternatives to access the single European entry point by traditional means.

Article 47 (9) requires the responsible Member States, or where applicable the requested Member State, to keep a record of the requests for correction or erasure of data and the decisions taken. The record has to be in the form of a written document and be made available to national supervisory authorities without delay. In line with Article 49, such authorities, designated pursuant to the GDPR, have to perform an audit of the national authorities' data processing operations at least every four years. Oversight helps to ensure

---

[82] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 17, 101, 105.

[83] *Ibid.*, pp. 104.

[84] See for example ICT's facts and figures, available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

a high level of protection of the rights of persons whose data are processed. Such a level of protection should be consistent and be of an equivalent level across all Member States.[85]

Improving procedures

According to Article 47 (2) of the proposals, the requested authorities will have to examine the request and reply in 45 days from the receipt of the request. Since the precarious situation can adversely affect the person concerned, the language should be made stronger to impose a duty to reply as soon as possible.

Article 47 (3) covers situations in which the requested Member State is not responsible for handling the request for correction or erasure of personal data. In such cases, the requested Member State will have to contact the authorities of the Member State responsible within seven days after the request has been lodged with its authorities. The Member State responsible will have to check the accuracy of the data and the lawfulness of the data processing within 30 days of such contact. Article 47 (3) does, however, not include any requirement to inform the person concerned about this procedure. The data subject will therefore not be aware who is dealing with his or her request.

Moreover, Article 47 (3) only refers to requests for "correction and erasure of personal data". It should also regulate the right to access in situations in which the requested Member State will not be responsible for the request to access personal data.

If, after an examination, the data stored in the Multiple-Identity Detector is found to be factually inaccurate or unlawfully recorded, the Member State responsible, or where applicable, the requested Member State must correct or delete it (Article 47 (4)). There is, however, no duty to inform the person about the correction made.

FRA opinion 24

To facilitate the right of access, correction and erasure of data processed through interoperability and avoid that data subjects have to navigate to find the right authority among the large number of Member States' authorities responsible, a streamlined system is needed.

The EU legislator should add a new provision to Chapter VII of the proposed Interoperability Regulations establishing an EU-wide request handling mechanism for all requests for access, correction and deletion of personal data. The EU-wide request handling mechanism should be tasked with providing information, logging the request and actions taken by the responsible authorities, forwarding the request to the responsible authority in the Member States, monitoring that the responsible authority responds, and offering a space where the concerned person could download the national authority's reply. eu-LISA could administer such a single European entry point and be tasked to prepare regular reports on the number of requests submitted, the response time and decision taken by the national authorities.

In addition, to increase the effectiveness of access, correction and erasure procedures, the EU legislator should:

- ***replace the time limit of 45 days in Article 47 (2) of the proposals with the wording "as soon as possible, and at the latest in 45 days";***
- ***cover in Article 47 (3) also requests for access to personal data;***

[85] GDPR, Recital 10.

- ***include in Article 47 (3) a duty to inform in writing any person who has approached a Member State other than the one responsible to review the request, indicating to whom the request has been forwarded;***
- ***add a provision in Article 47 (4) that a written confirmation on the correction or deletion should be sent to the data subject;***
- ***replace the reference to "the supervisory authority or authorities designated pursuant to Article 49 of Regulation (EU) 2016/679" in Article 49 (1) with "the supervisory authority" so as to cover also supervisory authorities designated to monitor the application of the Police Directive and to be consistent with Article 4 (4) of the proposals.***

Strengthening liability

The GDPR and the Police Directive contain the right to an effective judicial remedy against decisions taken by the supervisory authority,[86] the data controller or processor.[87] Individuals who suffered damage due to an infringement of the GDPR have the right to receive compensation from the controller or processor. Similarly, Member States are liable to provide compensation to individuals who suffered damage resulting from unlawful processing under the Police Directive or from any act infringing national provisions adopted pursuant to the Police Directive.[88]

The possibility to lodge an administrative complaint before a supervisory authority (Article 77 of the GDPR and Article 52 of the Police Directive) is not considered an effective remedy under Article 47 of the Charter.

Moreover, EU IT systems guarantee the right to bring a complaint before the courts or a competent authority.[89] If the person has suffered damage as a result of an unlawful processing operation or acts incompatible with the instruments, they must receive compensation from the Member State responsible for the damage suffered.[90] Such a provision is missing in the interoperability proposals.

FRA opinion 25

Although the EU data protection *acquis* applies in the context of interoperability, an explicit provision on the person's right to an effective remedy and on the Member States' liability for damages an individual might suffer would help promote a rights-compliant data processing for the purposes of interoperability.

The EU legislator should therefore include a provision establishing the individual's right to an effective remedy, drawing upon Articles 78 and 79 of the GDPR and Articles 53 and 54 of the Police Directive and respective provisions applying to the underlying IT systems.

---

86 GDPR, Art. 78; Police Directive, Art. 53.

87 GDPR, Art. 79; Police Directive, Art. 54.

88 GDPR, Art. 82; Police Directive, Art. 56.

89 VIS Regulation, Art. 40 (1); SIS II Regulation, Art. 43 (1); SIS II Decision, Art. 59 (1); SIS II proposal (police and judicial cooperation), Art. 66 (1); SIS II proposal (border checks), Art. 49 (1); SIS II proposal (return), Art. 13; EES Regulation, Art. 54 (1), Eurodac Regulation, Art. 29 (14) and (15), ECRIS-TCN proposal, Art. 25.

90 VIS Regulation, Art. 33; SIS II Regulation, Art. 48; SIS II Decision, Art. 64; SIS II proposal (police and judicial cooperation), Art. 70; SIS II proposal (border checks), Art. 53; SIS II proposal (return), Art. 13; EES Regulation, Art. 45, Eurodac Regulation, Art. 37, ECRIS-TCN proposal, Art. 18; Eurodac proposal, Art. 40.

The EU legislator should also include a provision on liability taking inspiration from Article 82 of the GDPR and Article 56 of the Police Directive and from the provisions included in the individual legal instruments regulating the respective EU IT systems.

10. Mainstreaming fundamental rights in implementation and evaluation

Creating a mechanism for fundamental rights oversight

Articles 49-51 of the proposals contain provisions for data protection oversight by national supervisory authorities as well as the EDPS. The duty to keep logs set out in Articles 10 (2), 16 (2), 24 (6) and 36 (3) intend to support their monitoring function. Logs can, however, only be used for data protection monitoring and not for monitoring, for example, the impact of interoperability on the right to non-discrimination or the rights of the child.

Similarly, the provisions on oversight in Articles 49-51 address only data protection, although interoperability may significantly impact on other fundamental rights. Cooperation between the national supervisory authorities and EU bodies, including relevant EU agencies, could promote a more holistic fundamental rights oversight, as a joint effort to evaluate the impact of interoperability on people's rights more broadly. A more effective mechanism to evaluate the impact *post factum* would also enable the European Commission, Member States or eu-LISA to take measures to address, for example, possible discriminatory effects of interoperability at an early stage. In addition, it could serve to increase the efficiency of interoperable systems.

FRA opinion 26

The proposals contain mechanisms to facilitate data protection oversight but less so for other fundamental rights, in particular non-discrimination. These could be strengthened.

The EU legislator should amend the wording in Articles 10 (2), 16 (2), 24 (6) and 36 (3) of the proposals extending the possibility to use the logs "only for data protection monitoring and monitoring the impact on fundamental rights".

The EU legislator could consider adding a provision to Article 51 on the cooperation between national supervisory authorities, European Data Protection Supervisor (EDPS) and other EU actors with fundamental rights expertise. This provision could be accompanied by a Recital indicating that the purpose of such cooperation is to strengthen the evaluation of the impact of interoperability on fundamental rights.

Mainstreaming fundamental rights during implementation

Chapters VIII and IX of the proposals contain provisions to facilitate their implementation. These provisions are also important vehicles to promote fundamental-rights compliance when putting interoperability into practice. FRA would like to focus in particular on four of them:

- Article 52 (4) establishes a *Programme Management Board* for the design and development phase. In its work the Board will likely be confronted with technical questions relating to fundamental rights and, more specifically, the protection of personal data. Article 52 (6) (d) gives the possibility to the Board to invite experts to its meetings but it does not contain any duty to have data protection expertise when discussing how to implement the different components of interoperability.
- Article 65 creates the *Interoperability Advisory Group* with tasks during the design and development phase as well as during the implementation phase of the future Interoperability Regulations. When advising on technical solutions or on different approaches to implement interoperability, the Interoperability Advisory Group must act in full compliance with the Charter. In light of the possible impact of

interoperability on the right to non-discrimination set out in Article 21 of the Charter and on the right to protection of personal data in Article 8 of the Charter, the Interoperability Advisory Group needs to have expertise in data protection as well as non-discrimination law.

- Article 66 entrusts eu-LISA to provide *training* on the technical use of the interoperability components. To reduce the risk of disproportionate interference with fundamental rights, the training eu-LISA provides should also include fundamental rights modules, as relevant in the context of interoperability. FRA can assist eu-LISA in developing these.
- Article 67 envisages that the European Commission develops a *Practical handbook* in close cooperation with Member States, eu-LISA and other relevant agencies. As observed in other policy areas – for example Eurosur or Returns – such handbooks are useful tools to promote fundamental rights compliant implementation of EU law. FRA stands ready to support the European Commission in mainstreaming fundamental rights when developing the Practical Handbook envisaged in Article 67.

FRA opinion 27

Provisions to facilitate the implementation of the proposed Interoperability Regulations should cover also fundamental rights.

To promote a fundamental rights compliant implementation of the interoperability components, the EU legislator should consider the following:

- ***include in Article 52 a duty for the Programme Management Board to invite an independent person with data protection expertise to its meetings, when they discuss agenda items which have a direct or indirect impact on the protection of personal data;***
- ***provide that the Interoperability Advisory Group established by Article 65 of the proposals include a person with proven fundamental rights expertise; and***
- ***expressly mention that the training to be provided by eu-LISA under Article 66 also covers fundamental rights and, in particular, the protection of personal data.***

Monitoring and evaluating the impact on fundamental rights

Article 68 regulates the monitoring and evaluation of the proposed Interoperability Regulations. This includes an evaluation report by the European Commission. Article 68 (5) (b) states that the evaluation report the European Commission has to produce must also cover the impact on fundamental rights. To operationalise this important provision, FRA stands ready to support the evaluation with its fundamental rights expertise.

To target a fundamental rights evaluation to the most relevant challenges in the field which, according to FRA, emerge in the implementation of interoperability, it would be useful to specify which rights such an evaluation should focus on.

Article 68 (8) requires Member States and Europol to collect and publish data on the effectiveness of interoperability for law enforcement purposes. The information and statistics listed in this provision is essential to evaluate the necessity and proportionality of using the data to prevent or combat serious crimes and terrorism. They cover a number of relevant points but do not include data on the use of interoperability in case of law enforcement actions concerning children. Such information would be useful to determine the proportionality of processing data on children but also to better illustrate if and how interoperability helps address child trafficking. Also, lit (c) of the provision requires to report

on the number of requests for access to the Common Identity Repository for law enforcement purposes, but without specifying whether the requests were granted by the central access point or not. Such information would be of significant use in order to assess the effectiveness of access to the data and of the access conditions.

Given that access to the Common Identity Repository envisaged in Article 20 also carries considerable fundamental rights challenges, the requirement to collect and publish data on the effectiveness of access should also apply to this mechanism. This could be developed taking Article 68 (8) as a starting point. Such information should be used to assess the effectiveness and fundamental rights impact of the provision.

FRA opinion 28

Article 68 regulates the monitoring and evaluation of the proposed Interoperability Regulations. As interoperability may result in reducing existing safeguards concerning law enforcement access to personal data and in a broader access to data by police for identification purposes, stronger *ex post* controls appear necessary.

The EU legislator should consider adding "in particular the right to protection of personal data, the right to non-discrimination, the rights of the child and the right to an effective remedy" to Article 68 (5) (b).

The EU legislator should consider requesting Member States and Europol to present separate statistics on child trafficking under Article 68 (8) (a) and to specify under Article 68 (8) (b) and (c) how many of the cases concern persons below 18 years of age. Under Article 68 (8) (c), the EU legislator should furthermore consider adding "with a breakdown between granted and rejected requests".

The EU legislator should also add a new paragraph to Article 68 listing a set of indicators for the use of interoperability in the context of Article 20. By analogy to Article 68 (8), this should include information and statistics including the exact purpose of the query, the number of queries including a breakdown between queries carried out with biometric, travel document and identity data, and the number and type of cases that have ended in successful identifications.

Annex 1: Identity data to be stored in the Common Identity Repository according to Article 18 (1)

	Legal instrument	EES Regulation	VIS Regulation	ETIAS Proposal	Eurodac proposal	ECRIS-TCN proposal
	Article(s) referred to	16 (1) (a)-(d), 17 (1) (a)-(c)	9 (4) (a)-(c), (5) & (6)	15 (2) (a)-(e)	13 (2) (a)-(e), (g) & (h)	Some data from Art. (5) (1) (a) + 5 (1) (b) & 5 (2)
NAME	Surname(s)and/or family name	O	O	O	O	O
NAME	First name(s) and/or given name(s) and/or forename(s)	O	O	O	O	O
NAME	Surname at birth		X	O		
	Name at birth				O	
	Former surname(s)		X			
	Previous names				O	X
	Alias(es)			X	O	X
	Pseudonyms(s)					X
	Artistic name(s)			X		
	Usual name(s)			X		
BIRTH	Date of birth	O	O	O	O	O
BIRTH	Place of birth		X	O	O	O
BIRTH	Country of birth		X	X		X
	Nationality(ies)	O	O	O	O	O
	Nationality at birth		X			
	Sex or gender	O	O	O	O	O
	First name(s) of parents			X		
TRAVEL DOCUMENT (TD)	Type and number of TD(s)	X	X	X	X[a]	
TRAVEL DOCUMENT (TD)	*Authority issuing the TD*		*X*[b]			
TRAVEL DOCUMENT (TD)	Country issuing TD			X		
TRAVEL DOCUMENT (TD)	3 letter code of the issuing country	X	X[b]		X	
TRAVEL DOCUMENT (TD)	*Issuance date*		*X*[b]			
	Expiry date/validity	X	X	X	X	
	Facial image	X	X[b]		X	X
	Fingerprints	X[c]	X		X	X[d]
	Photograph		X[b]			

Notes: **O**: *identity data as defined in Art. 4 (9)*
X: *other data included in Art. 18 (1)*

[a] *or identity document*

[b] *changes introduced with the proposed amendments to the VIS Regulation (Article 55d of the interoperability proposal in the field of borders and visa). VIS currently contains a photograph. The interoperability proposal will amend Article 9 (5) of the VIS Regulation and replace the photograph with a facial image. The authority issuing the travel document and its date of issue (included in the table in italics) will be moved to Art. 9 (4) (cc), therefore they will be not stored in CIR. Article 9 (4) (b) will include the three-letter code of the issuing country of the travel document or documents.*

[c] *only for visa-exempt third-country nationals*

[d] *including the reference number of the fingerprint data of the convicted person including the code of the convicting Member State*

Source: FRA, 2018

TK-01-18-396-EN-N

Publications Office

ISBN: 978-92-9474-022-9
doi: 10.2811/123362

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

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