

FRA Opinion – 3/2018
[Security features ID]

Vienna, 5 September 2018

Fundamental rights implications of storing biometric data in identity documents and residence cards

Opinion of the
European Union Agency for Fundamental Rights

Contents

- Opinions 5
- Introduction 8
- 1. **Avoiding that biometrics are also stored in national databases**..... 12
 - FRA Opinion 1..... 14
- 2. **Ensuring a fundamental rights compliant implementation**..... 16
 - FRA opinion 2 17
- 3. **Processing the minimum necessary biometric data** 19
 - FRA Opinion 3..... 20
- 4. **Respecting human dignity when collecting biometric data**.....21
 - FRA Opinion 4.....21
- 5. **Collecting biometric data from children**22
 - FRA Opinion 5..... 23
- 6. **Collecting biometric data from older persons and persons with disabilities**23
 - FRA Opinion 6..... 25

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 (EC) No. 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 (EC) No. 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 (EC) No. 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 FRA opinion on the proposed Regulation on the European Travel Information and Authorisation System,³ and FRA opinion on the revision of the Visa Information System.⁴

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

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 (2018), [Opinion of the European Union Agency for Fundamental Rights on the revised Visa Information System and its fundamental rights implications](#), FRA Opinion – 2/2018 [VIS], Vienna, 30 August 2018.

interoperability of EU information systems: borders and security'⁵ as well as on the findings of the FRA research project on the processing of biometric data in large-scale information technology systems established by the European Union to manage asylum and migration published on 28 March 2018,⁶

Having regard to the request of the European Parliament of 21 August 2018 to FRA for an opinion "on the fundamental rights implications of the Commission proposal on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (2018/0104 (COD))' and among others on the right to the protection of personal data",

SUBMITS THE FOLLOWING OPINION:

⁵ FRA (2017), [Fundamental rights and the interoperability of EU information systems: borders and security](#), Luxembourg, Publications Office, July 2017.

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

Opinions

FRA Opinion 1

The creation of national dactyloscopic databases of all identity and residence cards holders would constitute a grave interference with the right to respect for private and family life (Article 7 of the Charter) and with the right to protection of personal data (Article 8 of the Charter). There is no analysis which would demonstrate the necessity and proportionality of such grave interference. Whereas the proposal does not provide a legal basis for setting up or maintaining national databases, it could be clearer in ensuring that Member States do not use the biometric data collected for the purposes of the regulation to feed national biometric databases – at least as long as the proportionality and necessity of such processing is demonstrated in light of the strict requirements established by the EU data protection *acquis*.

The EU legislator should add a Recital explicitly indicating that the biometric data collected for the purpose of this Regulation should not be stored in national databases covering identity cards or residence cards holders.

In addition, as recommended by the European Data Protection Supervisor, the EU legislator should expressly provide in Article 9 of the proposal for the immediate deletion of the biometric data collected once they are stored in the chip.

FRA opinion 2

Several provisions of the proposal impact on fundamental rights. In addition to those provisions which introduce limitations to fundamental rights (first of all the right to respect for private and family life and the right to protection of personal data), fundamental rights violations may also emerge during the implementation of provisions which in itself are compatible with the EU Charter. In the proposal, reference to fundamental rights in general is confined to a recital.

To promote a fundamental rights compliant implementation, the EU legislator should include a general fundamental rights safeguard clause in the operative part of the Regulation, drawing upon Recital (23) of the proposal. Such a clause should focus on the implementation, for example by saying “When implementing this Regulation Member States shall respect the fundamental rights and observe...” and mention other fundamental rights which might be particularly affected by the proposal in its implementation, such as human dignity, the right to the integrity of the person, the prohibition of inhuman or degrading treatment, the right to equality before the law and non-discrimination, the rights of the child and the rights of the elderly.

The EU legislator should clarify in Recital (21) and Article 12 (1) respectively whether the report on the implementation of the Regulation should be issued three or four years after its date of application. The EU legislator should add a sentence to Article 12 (1) stipulating that “the report shall also examine whether the implementation is compliant with the data collection purposes listed in Article 10 (3).”

The EU legislator should add in Article 12 (2) a provision indicating that the Commission’s evaluation should assess the fundamental rights impact of the Regulation.

FRA Opinion 3

The proposal suggests to store the facial image as well as two fingerprints of the holder of an identity card. This solution is not supported in the impact assessment, which concludes that the purpose can be achieved by limiting the compulsory storage to facial images. In case the EU legislator follows the proposal and thus departs from the findings of the Commission's impact assessment, the necessity and proportionality of processing two biometric identifiers needs to be carefully re-assessed.

The EU legislator must thoroughly assess the necessity of processing and storing two types of biometric identifiers of EU nationals in national identity cards, in case it decides to follow the Commission proposal. In addition to the elements considered by the European Commission in its impact assessment, the EU legislator should also take into account possible risks that biometric data may be unlawfully accessed, including by criminals who may use such data stored on a lost or stolen identity document to cast a fake set of fingerprints.

FRA Opinion 4

The safeguard to respect human dignity in case there are difficulties in collecting biometric identifiers only applies to identity cards and not to residence cards. This asymmetry is not justified.

The EU legislator should move the second paragraph of Article 4 to Chapter V which includes common provisions, so that the safeguard included therein also applies when Member States collect biometric identifiers from third-country national family members of EU citizens to issue their residence cards and permanent residence cards in the new format.

FRA Opinion 5

Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions that public authorities and private actors take in relation to children. This implies that when children's biometric data are exceptionally stored, these should not adversely affect them, including by exposing them to a heightened risk of wrong matches. Furthermore, there should be an operational clause obliging relevant authorities to collect fingerprints in a child-sensitive and gender-sensitive manner.

The EU legislator should move the content of Recital (11) to the operative part of the Regulation (for example under Chapter V on common provisions), stipulating that the collection of biometric identifiers should be undertaken in a child-sensitive and in a gender-sensitive manner.

To avoid the risk of wrong matches, the EU legislator should set the minimum age of storing fingerprints for children in residence cards for third-country national family members at 12 years – the minimum fingerprinting age set for identity cards. Alternatively, the EU legislator should require that any match concerning children carried out with biometric identifiers taken more than five years before should be subject to a compulsory manual check by a dactyloscopic expert.

FRA Opinion 6

The proposal includes a reference to the rights of persons with disabilities but such reference does not mention the relevant article of the Charter. Under Article 25 of the Charter, older people have the right to lead a life in dignity and independence and to

participate in social and cultural life. The life-expectancy is increasing and older people are increasingly mobile. The Regulation could better reflect this reality.

The EU legislator should reformulate Recital (13) of the proposal to read “When implementing this Regulation EU Member States should respect the obligations....” adding also a reference to Article 26 of the Charter.

To avoid the risk of wrong matches, the EU legislator should avoid compulsory storage of fingerprints of people older than 70 years. Alternatively, the EU legislator should require that any match concerning people aged 70 years or older must be subject to a compulsory manual check by a dactyloscopic and/or facial image expert.

Introduction

This Opinion by the European Union Agency for Fundamental Rights (FRA) aims to inform the European Parliament's position concerning the legislative proposal for a Regulation on strengthening the security of identity cards of European Union (EU) citizens and of residence documents issued to EU citizens and their family members exercising their right of free movement.⁷ It focuses on the processing of biometric data and complements the opinion published by the European Data Protection Supervisor (EDPS).⁸

The right to free movement within the EU

EU citizens and their family members (regardless of their nationality) enjoy the right to move and reside freely within the EU. Such right is guaranteed in Article 45 of the EU Charter of Fundamental Rights (hereinafter: 'the Charter') and in Articles 20-21 of the Treaty on European Union (TEU). The same right is conferred to nationals of Iceland, Liechtenstein, Norway and Switzerland.⁹ While this Opinion refers to 'EU citizens' affected by the proposed Regulation, the proposal, in particular Chapters III-V, equally affects nationals of Iceland, Liechtenstein, Norway and Switzerland who made use of free movement rights, and their third-country national family members.

The right to free movement within the EU is one of the main achievements of the European integration, giving all Union citizens the right to travel, live and work wherever they wish within the European Union. The Free Movement Directive (Directive 2004/38/EC) regulates such right in detail.¹⁰ FRA just published an EU-wide comparative overview of the application of the Directive 2004/38/EC across the Member States based on a review of case law at national level.¹¹

Articles 4 and 5 of the Free Movement Directive provide for the right of EU citizens and their family members to exit and enter EU Member States with a valid identity card or a passport.

All Union citizens have the right of residence on the territory of another Member State for a period of more than three months, if they fulfil the conditions set out in Article 7 of the Free Movement Directive. The directive also confers this right to their family members, including those who are third-country nationals.

When **EU nationals** exercise their free movement rights, for example, by moving to another Member State to work, study or live there for more than three months, they may be required to register with the authorities (Article 8 of the Free Movement

⁷ European Commission (2018), [Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement](#), COM(2018) 212 final - 2018/0104 (COD), Brussels, 17 April 2018.

⁸ European Data Protection Supervisor (2018), [EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents](#), 10 August 2018.

⁹ See [Agreement on the European Economic Area](#), 2 May 1992, Part III, Free Movement of Persons, Services and Capital, OJ 1994 L1. For Switzerland, see [Agreement between the European Community and its Member States, on the one part, and the Swiss Confederation, on the other, on the free movement of persons](#), signed in Luxembourg on 21 June 1999, entered into force on 1 June 2002, OJ 2002 L 114/6.

¹⁰ [Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation \(EEC\) No. 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC \(Text with EEA relevance\)](#), OJ L 2004 158/77.

¹¹ FRA (2018), [Making EU citizens' rights a reality: national courts enforcing freedom of movement and related rights](#), Luxembourg, Publications Office of the European Union, August 2018.

Directive). In such case, they must be issued with a “**registration certificate**” and after a certain period of time (five consecutive years), a document certifying permanent residence under Article 19 of the directive (if they fulfil the relevant conditions).

For third-country family members such registration with the authorities is compulsory. Under Articles 10 and 20 of the Free Movement Directive, Member States are under an obligation to issue “**residence cards**” for periods of residence exceeding three months and after a certain period of time (five consecutive years), “permanent residence cards” to **third-country national family members of EU citizens who have exercised free movement rights**. According to Article 5 (2) of the directive, read in conjunction with its Article 3, holders of such residence cards are entitled to cross the border without a visa (in case they come from a country subject to visa requirements), if they accompany or join their EU citizen family member.

The background to the legislative proposal

The impact assessment to the Commission’s proposal describes different challenges faced by EU citizens and third-country national family members who made use of their free movement rights when they use their national identity cards or residence cards in another EU Member State. It notes that such challenges are, at least to some extent, the result of the large diversity of identity cards in use.¹²

Complications emerge also when EU nationals use identity cards or when third-country nationals use residence cards issued under the Free Movement Directive to cross the external borders of the Schengen area (and internal borders, in case of temporary re-introduction of border checks). This can occur in the following circumstances:

- Based on bilateral agreements, EU nationals can use identity cards (instead of their passports) to travel to a number of non-EU countries, for example, in the Western Balkans.
- Third-country nationals who are family members of EU citizens who exercise free movement rights and who would normally require a visa to enter the EU may cross the border with their passport together with their “residence card” when they accompany or join an EU citizen family member. The residence card thus replaces the need for a visa.

Weak security features of some of these documents have led to the use of fraudulent identity cards and residence cards. Persons travelling with such cards may be suspected of fraud and, as a result, face problems when crossing the border, particularly if they present identity cards or residence cards which have weak security features.¹³

For the national authorities, weak security features in documents which entitle the holder to access the Schengen area pose challenges to the internal security of the

¹² European Commission (2018), [*Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement*](#), SWD/2018/110 final, Strasbourg, 17 April 2018 (*Impact Assessment*), pp. 10, 21. See also Tables 2.1 and 2.2 on pp. 103-105.

¹³ Impact Assessment, pp. 12-14.

Member States.¹⁴ According to the European Commission, document forgery is one of the typical cases of fraud related to the Free Movement Directive.¹⁵

The proposal

Identity cards facilitate – beyond border crossing – interactions with public authorities for many aspects of life, e.g. taxation, employment, education, etc.

The proposal envisages

- to approximate the format of identity cards issued to EU Member States' own nationals, registration certificates issued to EU nationals who exercise free movement rights and of residence cards issued to third-country nationals who are family members of EU citizens;
- to enhance security features of these identity cards and residence cards. In essence, the proposal suggests to include a chip storing the facial image as well as two fingerprints of the holder in these two types of cards.

Fingerprints and facial images are the two types of biometric identifiers which are mostly used in the EU to verify the identity of a person.¹⁶ Biometrics allow for the identification of an individual through one or more unique factors specific to the physical identity of a person.¹⁷

These two measures, combined with multilingual information on their title and content (Articles 3 (2) and 6 (a)), would increase the reliability and acceptance of such documents in cross-border situations, i.e. when crossing the border or when using the document for different purposes in another EU Member State.

Although increased acceptance of these documents may partly be achieved by an approximation of their visible appearance, the suspicion that an individual is trying to cross the border with false or forged documents (and the inconveniences associated with it an individual may face) can only be reduced by enhancing security features of identity and residence cards. Thus, the authorities as well as the individual would benefit from upgraded security features.

¹⁴ Impact Assessment, pp. 11-12, 17; European Commission (2016), [Communication from the Commission to the European Parliament, the European Council and the Council. Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders](#), COM(2016)602 final, Brussels, 14 September 2016, p. 10; Council of the European Union (2017), [Council conclusions on the EU Citizenship Report 2017 \(adoption 11 May 2017\)](#), Brussels, 11 May 2017, p. 5.

¹⁵ European Commission (2013), [Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Free movement of EU citizens and their families: Five actions to make a difference](#); Commission of the European Communities (2009), [Communication from the Commission to the European Parliament and the Council on guidance for better transposition and application of Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States](#), COM(2009) 313 final, Brussels, 2 July 2009, p. 15.

¹⁶ See FRA (2018), [Under watchful eyes biometrics, EU IT systems and fundamental rights](#), pp. 25-26 as well as Table 1: Existing and planned EU large-scale IT systems, page 23, for an overview of biometric identifiers used by the EU in large scale IT systems.

¹⁷ See, for example, Jain, A.K., Bolle, R.M. and Pankanti, S. (eds.) (2006), *Biometrics – Personal Identification in Networked Society*, New York, Springer, 2006, pp. 1-42.

Impact on fundamental rights

As noted in the Commission's impact assessment, the proposal impacts on several fundamental rights (see for more details Chapter 2), which the Commission has thoroughly analysed.¹⁸

To address risks to fundamental rights identified in the Commission's impact assessment, the proposal contains several safeguards. These include, for example, the duty to ensure that human dignity is respected when difficulties arise in taking fingerprints for identity cards (proposed Article 4). Recitals (11) and (13) respectively make references to children and people with disabilities included in the proposal. Article 10 contains rules on the protection of personal data.

The FRA Opinion

Most points in this FRA Opinion relate to risks to fundamental rights which may result from the implementation of the regulation.

This opinion mainly focuses on the processing of biometric data in identity cards issued by EU Member States to their own nationals and residence cards issued to third-country family members of EU nationals exercising free movement rights.

FRA hereby present six individual opinions addressing the following points:

- Avoiding that biometrics are also stored in national databases;
- Ensuring a fundamental rights compliant implementation;
- Processing the minimum necessary biometric data;
- Respecting human dignity when collecting biometric data;
- Collecting biometric data from children;
- Collecting biometric data from elderly and persons with disabilities.

¹⁸ Impact Assessment, see Section 6 (policy options), in particular pp. 32, 33, and Section 8 (on preferred option), in particular, pp. 59-61.

1. Avoiding that biometrics are also stored in national databases

Article 10 (3) of the proposal – which applies to both types of documents (identity cards and residence cards) – states that biometric data collected and stored in the chip (i.e. the facial image and the two fingerprints) can only be used in accordance with Union and national law for the following purposes:

- to verify the authenticity of the document or
- to verify the identity of the holder, by means of directly available comparable features when the identity card or residence card is required to be produced by law.

Article 10 (2) of the proposal stipulates that “[i]nformation in machine-readable form shall only be included in an identity card or residence document in accordance with this Regulation or the national legislation of the issuing Member State”.

As underlined by the EDPS, personal data must be processed only for the legitimate purpose for which the data was originally collected.¹⁹ Clearly, proposed Article 10 (2) and (3) does not give to EU Member States a legal basis to use the collected biometrics to set up a national database of identity card holders which would store facial images and/or fingerprints.²⁰ At the same time, the proposal does also not exclude that Member States make use of the biometric data they will be obliged to collect under EU law to establish or enhance national dactyloscopic databases.

The wording in the proposal is similar to Article 4 (3) of Regulation (EC) No. 2252/2004 (as amended) on passports, which also defines that the collected biometrics can only be used to verify the authenticity of the passport and the identity of the holder. Nevertheless, some EU Member States have considered storing the biometric data in databases, as a recent judgement by the Court of Justice of the EU shows.²¹ As noted by the CJEU, setting up or maintaining national databases storing data, including biometrics, of their own nationals falls exclusively under the competence of Member States.²²

Some EU Member States maintain different national databases, some of which also cover EU nationals and/or third-country nationals who are family members of persons exercising free movement rights. For example, in Estonia the regulation on Statutes of the Identity Documents Database provides for the storage of biometrics (facial image, fingerprints) of, among others, passport holders, for up to 50 years.²³ In Finland, Article 29 of the Law on Passport establishes a passport register which contains facial images and fingerprints and to which various authorities, including law enforcement

¹⁹ EDPS (2018), [EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents](#), 10 August 2018, para. 42.

²⁰ The CJEU explained in regard to passports that Art. 1 (2) of Regulation (EC) No. 2252/2004 (containing a similar wording as Art. 3 (3) and (4) of the proposal) “does not provide for the storage of fingerprints except within the passport itself” (para. 60). See CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013, paras. 54- 63.

²¹ CJEU, Joined cases C-446/12 to C-449/12, *W.P. Willems and others v. Burgemeester van Nuth and Others*, 16 April 2015.

²² *Ibid.*, para. 47.

²³ Estonia, Statutes of the Identity Documents Database ([Isikut tõendavate dokumentide andmekoogu pidamise põhimäärus](#)), adopted on 18 December 2015 and established on the basis of “Identity Documents Act” ([Isikut tõendavate dokumentide seadus](#)), Arts. 6, 7, 16 (2) on access and 18 (on retention time).

authorities and embassies abroad have access.²⁴ In the Netherlands, the creation of a national database of passport holders was considered in the past.²⁵ In Slovakia, biometric data contained in the travel document (facial image and fingerprints) are also stored in travel document databases managed by the issuing authorities (local police authorities in case of regular passports) as well as in a central database managed by the Ministry of the Interior. The law limits the use of the biometric data in the travel document itself to verifying the validity of the document and establishing the person's identity, but the travel document databases can be directly accessed by the Police to carry out its competences.²⁶

Member States could see the duty to process fingerprints and facial images established by EU law for identity and residence cards as an opportunity to store the collected biometrics also in national databases. This would result in a breach of the principle of purpose limitation included in Article 8 of the Charter and further specified in Article 5 (1) (b) of the General Data Protection Regulation (GDPR). According to the GDPR, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". The creation of national dactyloscopic databases would constitute a much graver interference with the right to respect for private and family life (Article 7 of the Charter) and with the right to protection of personal data (Article 8 of the Charter and Article 16 of the Treaty of the Functioning of the EU (TFEU)) as the simple storage of biometrics in a chip. Such interference would have to be subject to a separate necessity and proportionality assessment.

The impact of national databases containing searchable fingerprints or facial images and the fundamental rights risks associated with it must also be examined in light of EU efforts to make existing and planned EU IT systems interoperable.²⁷ The Explanatory Memorandum notes that the proposal will benefit also the exchange of information through interoperability, including for conducting identity checks by competent authorities within the territory of EU Member States.²⁸ In future, an officer who is authorised to query EU-wide IT systems will be able to do this using a single search interface (the European Search Portal – ESP) carried out with alphanumeric and/or biometric data (using the shared Biometric Matching Service – BMS). According to the different legislative proposals, personal data of virtually all third-country nationals – ranging from short-term visitors to long-term residence status holders – will be stored in one or more Europe-wide IT systems. In addition, the Schengen Information System also stores data of some categories of EU nationals (i.e. missing persons, persons

²⁴ Finland, Law on Passports (*Passilaki*), 671/2006, Art. 29.

²⁵ CJEU, Joined cases C-446/12 to C-449/12, *W.P. Willems and others v. Burgemeester van Nuth and Others*, 16 April 2015, paras. 14-15.

²⁶ Slovakia, Act No. 647/2007 Coll. on Travel Documents (*Zákon o cestovných dokladoch a o zmene a doplnení niektorých zákonov*), Arts. 5 and 29.

²⁷ European Commission (2018), [Amended 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, Regulation \(EU\) 2017/2226, Regulation \(EU\) 2018/XX \[the ETIAS Regulation\], Regulation \(EU\) 2018/XX \[the Regulation on SIS in the field of border checks\] and Regulation \(EU\) 2018/XX \[the eu-LISA Regulation\]](#), COM(2018) 478 final, Brussels, 13 June 2018; European Commission (2018), [Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems \(police and judicial cooperation, asylum and migration\) and amending Regulation \(EU\) 2018/XX \[the Eurodac Regulation\], Regulation \(EU\) 2018/XX \[the Regulation on SIS in the field of law enforcement\], Regulation \(EU\) 2018/XX \[the ECRIS-TCN Regulation\] and Regulation \(EU\) 2018/XX \[the eu-LISA Regulation\]](#), COM(2018) 480 final, Brussels, 13 June 2018.

²⁸ Explanatory Memorandum, p. 3.

wanted for arrest, persons sought to assist with a judicial procedure and persons for discreet checks or specific checks).²⁹

Once European IT systems are made interoperable, Member States could establish a search function under domestic law which could allow to search for a person simultaneously in their national systems as well as in the EU IT systems. Where IT systems or databases store fingerprints and/or facial images, these searches could be carried out using biometrics. In such a way, relevant national authorities would have access to a large pool of fingerprints and/or facial images.

The establishment of a central national database would also increase the risk of abuse for using the data for other purposes than those originally intended. Due to its scale and the sensitive nature of the data which would be stored, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights.

The risks connected to such broad search possibilities are different depending on whether the databases store facial images or fingerprints. Fingerprint searches can only be carried out if the person is present, if the officer has a document with stored fingerprints, or if “latent fingerprints” collected on a crime scene are available. In contrast, for facial image searches, the picture can be taken from various sources, provided it is of sufficient quality. It could come from individual paper files, evidence gathered during investigations but also from social media or closed circuit cameras (CCTV). Already in 2012, the Article 29 Data Protection Working Party of the EU Council, in its opinion on the development of biometric technologies, underlined the potential risks of using facial images “for covert surveillance by law enforcement authorities to identify potential troublemakers”.³⁰

FRA Opinion 1

The creation of national dactyloscopic databases of all identity and residence cards holders would constitute a grave interference with the right to respect for private and family life (Article 7 of the Charter) and with the right to protection of personal data (Article 8 of the Charter). There is no analysis which would demonstrate the necessity and proportionality of such grave interference. Whereas the proposal does not provide a legal basis for setting up or maintaining national databases, it could be clearer in ensuring that Member States do not use the biometric data collected for the purposes of the regulation to feed national biometric databases – at least as long as the proportionality and necessity of such processing is demonstrated in light of the strict requirements established by the EU data protection *acquis*.

The EU legislator should add a Recital explicitly indicating that the biometric data collected for the purpose of this Regulation should not be stored in national databases covering identity cards or residence cards holders.

²⁹ [Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System \(SIS II\)](#), OJ L 205/63 (*SIS II Decision*), Art. 26 (persons wanted for arrest), Art. 32 (missing persons), Art. 34 (persons sought to assist with a judicial procedure), Art. 36 (persons for discreet checks or specific checks).

³⁰ Article 29 Data Protection Working Party (2012), [Opinion 3/2012 on developments in biometric technologies](#), 00720/12/EN, WP193, 27 April 2012, p. 22.

In addition, as recommended by the European Data Protection Supervisor, the EU legislator should expressly provide in Article 9 of the proposal for the immediate deletion of the biometric data collected once they are stored in the chip.

2. Ensuring a fundamental rights compliant implementation

Including a horizontal fundamental rights safeguard clause

The Commission's impact assessment as well as the proposal itself give considerable attention to fundamental rights. Nevertheless, to promote a fundamental rights compliant implementation of the new rules, stronger provisions are needed.

Recital (23) of the proposal stipulates that the Regulation "respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the respect for private and family life, the right to the protection of personal data, the right to free movement and the right to an effective remedy." While the whole proposal needs to be read in the light of the respective recitals, stronger safeguards are needed to address the various fundamental rights risks which may emerge during the implementation of the Regulation. This is for two important reasons.

First, the recital's formulation points out only some of the relevant fundamental rights at stake, namely the respect for private and family life, the right to the protection of personal data, the right to free movement and the right to an effective remedy. The proposal might significantly affect also other fundamental rights protected by the Charter, such as the right to human dignity (Article 1), the right to the integrity of the person (Article 3), the prohibition of inhuman or degrading treatment (Article 4), the right to equality before the law (Article 20) and non-discrimination (Article 21), the rights of the child (Article 24) and the rights of the elderly (Article 25), as illustrated with the following two examples.

- The physical impossibility to provide fingerprints or a facial image could result in discrimination or unequal treatment, for example on the basis of age or disability (in case of a deformed face or hand after an accident). The inclusion of an explicit clause providing for their exemption from the requirement to provide fingerprints in proposed Article 3 (5) (b) represents an important safeguard to guarantee the rights protected by Articles 20 and 21 of the Charter. Nevertheless, an explicit reminder to these two Charter rights would further enhance the protection of persons unable to provide fingerprints or facial image, whose number may be significant.³¹
- In exceptional cases, Member States' authorities may resort to coercive measures to oblige an individual to provide his or her fingerprints, in particular in cases of mandatory identity cards. Excessive use of force would interfere with the prohibition of inhuman or degrading treatment or punishment in Article 4 of the Charter from which no derogations are possible and/or with the right to integrity of the person protected by Article 3 of the Charter.

Second, the reference to the protection of fundamental rights is currently included in a recital, which helps to interpret the provisions but does not constitute an enforceable

³¹ For example, according to eu-LISA, based on reports by 11 Member States, between October 2015 and September 2017, 253,684 visa applicants out of the 31,359,706 visa applicants in total were registered without fingerprints on factual grounds, which represents about 0.81 % of all applicants. See eu-LISA (2018), [Technical reports on the functioning of VIS as per Article 50\(3\) of the VIS Regulation and Article 17\(3\) of the VIS Decision](#), May 2018, p. 28. Given that the proposal will affect about 370 million potential ID card holders (Impact assessment, Annex 8), millions of citizens might be unable to provide fingerprints.

legal rule in itself.³² Although the Charter must be respected in all matters falling under EU law (Article 51 of the Charter), an explicit fundamental rights safeguard clause in the operative part of the regulation would promote a more comprehensive fundamental rights compliant implementation of the regulation in practice. For example, a provision addressing the respect for fundamental rights when collecting biometric identifiers for passports is included in Article 1a (2) of the EU Passport Regulation as amended by Regulation (EC) No. 444/2009.³³

Evaluating the impact on fundamental rights

Pursuant to Article 12 (1) of the proposal, the Commission will have to report on the implementation of the Regulation to the European Parliament, the Council and the European Economic and Social Committee four years after its date of application. The timing of the report remains, however, unclear, since, according to Recital (21), it should be issued three years after the date of application whereas Art 12(1) refers to four years. Both provisions do generally not prescribe the content of the report. Recital (21) only stipulates that the report should cover the “appropriateness of the level of security”.

The implementation report presents a good opportunity to assess whether the collected data is processed for the purposes envisaged in the proposal as explained in Chapter 1 or whether it has led to unintended fundamental rights consequences.

In addition, under proposed Article 12 (2) the Commission will have to prepare an evaluation of the Regulation six years after its date of application, which will have to be in line with the Commission’s Better Regulation Guidelines.³⁴ These guidelines do not sufficiently address the need to evaluate the fundamental rights impacts. Since the proposed regulation might significantly affect fundamental rights, as described in other sections of this Opinion, a thorough evaluation of this aspect would be needed.

FRA opinion 2

Several provisions of the proposal impact on fundamental rights. In addition to those provisions which introduce limitations to fundamental rights (first of all the right to respect for private and family life and the right to protection of personal data), fundamental rights violations may also emerge during the implementation of provisions which in itself are compatible with the EU Charter. In the proposal, reference to fundamental rights in general is confined to a recital.

To promote a fundamental rights compliant implementation, the EU legislator should include a general fundamental rights safeguard clause in the operative part of the Regulation, drawing upon Recital (23) of the proposal. Such a clause should focus on the implementation, for example by saying “When implementing this Regulation Member States shall respect the fundamental rights and observe...” and mention other fundamental rights which might be particularly affected by the proposal in its

³² CJEU, Case 215/88, *Casa Fleischhandels-GmbH v. Bundesanstalt für landwirtschaftliche Marktordnung*, 13 July 1989, para. 31: “Whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule.”

³³ [Regulation \(EC\) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation \(EC\) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States](#), OJ L 142/1. Art. 1a (2) of the amended regulation stipulates that: “Member States shall collect biometric identifiers from the applicant in accordance with the safeguards laid down in the Council of Europe’s Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child. Member States shall ensure that appropriate procedures guaranteeing the dignity of the person concerned are in place in the event of there being difficulties in enrolling.”

³⁴ European Commission (2017), [Better Regulation Guidelines](#), SWD(2017) 350 final, Brussels, 7 July 2017.

implementation, such as human dignity, the right to the integrity of the person, the prohibition of inhuman or degrading treatment, the right to equality before the law and non-discrimination, the rights of the child and the rights of the elderly.

The EU legislator should clarify in Recital (21) and Article 12 (1) respectively whether the report on the implementation of the Regulation should be issued three or four years after its date of application. The EU legislator should add a sentence to Article 12 (1) stipulating that “the report shall also examine whether the implementation is compliant with the data collection purposes listed in Article 10 (3).”

The EU legislator should add in Article 12 (2) a provision indicating that the Commission’s evaluation should assess the fundamental rights impact of the Regulation.

3. Processing the minimum necessary biometric data

Article 3 (3) and Article 7 (1) of the proposal oblige EU Member States to collect and store a facial image and two fingerprints in interoperable formats on the identity cards and residence cards they issue. Pursuant to proposed Article 3 (3), the biometric data will be stored in a “highly secure” chip which is included in the document itself.

The main question is whether the proposed inclusion of two biometric identifiers, namely facial image and fingerprints, is necessary to address abuse and reduce inconveniences and troubles for the holders by confirming that they are the genuine holders of the document.

The impact assessment notes that forgery, counterfeiting as well as related practical difficulties for the holders of the documents are more frequent with documents which do not contain biometric identifiers.³⁵ Currently, there is no EU law requirement for the format and security features of these two types of documents. The only exception is Article 5a of Council Regulation (EC) No. 1030/2002 (as amended), which establishes a uniform format for residence permits for third-country nationals and allows that such uniform format be used also for other purposes, provided this does not create confusion. This means that the uniform format under this regulation – which under its Article 4a includes the facial image and two fingerprints of the holder – can be used also for (permanent) residence cards issued under Articles 9 and 20 of the Free Movement Directive.³⁶ In fact, according to the European Commission, 12 Member States use the common format for residence permits issued to third-country nationals under Council Regulation (EC) No. 1030/2002 (as amended) for the format of residence cards issued to third-country national family members.³⁷

In the absence of minimum standards presently set in EU law, practices vary considerably among EU Member States according to the Commission’s impact assessment:

- Identity cards: all EU Member States except Denmark and the United Kingdom issue identity cards to their own nationals. There are about 86 different types of identity cards in circulation.³⁸ Roughly, half of the EU Member States issued identity cards with biometric features (facial image and/or fingerprints).³⁹
- Residence cards under Articles 9 and 20 of the Free Movement Directive: 15 EU Member States issued plastic cards storing biometric data.⁴⁰

³⁵ Impact Assessment, pp. 12-14.

³⁶ See [Council Regulation \(EC\) No. 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals](#), OJ L 157/1 as amended by [Council Regulation \(EC\) No. 380/2008 of 18 April 2008 amending Regulation \(EC\) No. 1030/2002 laying down a uniform format for residence permits for third-country nationals](#), OJ L 115/1 and by [Regulation \(EU\) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation \(EC\) No. 1030/2002 laying down a uniform format for residence permits for third-country nationals](#), OJ L 286/9. The relevant provision introducing Articles 4a-4b and 5a is in the 2008 amendments.

³⁷ Impact Assessment, p. 12.

³⁸ Centre for Strategic and Evaluation Services (2017), [Study to Support the Preparation of an Impact Assessment on EU Policy Initiatives on Residence and Identity Documents to Facilitate the Exercise of the Right of Free Movement](#), 28 August 2017, p. ii.

³⁹ Impact Assessment, pp. 21, 104-5 (Table 2.2).

⁴⁰ Impact Assessment, p. 107-108 (Table 2.3).

For identity cards, Article 3 (3) of the proposal aligns biometric data with those of passports.⁴¹ For residence cards of family members, Article 7 of the proposal aligns them to those residence permits of third-country nationals who do not enjoy free movement rights.

For identity cards issued to EU Member States' own nationals, the impact assessment does not contain sufficient justification for the mandatory collection of facial images and fingerprints. In fact, it concludes that the objective could be achieved by less intrusive means, namely by requiring only the mandatory collection of facial images, leaving the collection of fingerprints optional.⁴² The Commission correctly noted that the standards applicable to passports, i.e. a facial image and two fingerprints, under Regulation (EC) No. 2252/2004 (as amended) are not automatically justified for identity cards.⁴³ Although the lawfulness of storing such data in passports was confirmed by the CJEU in *Schwarz*, it should be borne in mind that the Court assessed the proportionality of limiting the right to respect for private and family life and the right to data protection against the aims of preventing falsification and fraudulent use of passports and, by extension, the objective of preventing irregular entry into the EU.⁴⁴

National identity cards, unlike passports, are not primarily used for crossing the external border.⁴⁵ EU nationals mainly use identity cards for interactions with the administration, banks and other private actors in their own country and to move across borders within the Schengen area, without being subject to border checks. Therefore, the necessity of processing the same biometric identifiers as in passports is not automatically justified in light of the CJEU's above case law. As pointed out by the European Data Protection Supervisor, the inclusion of facial images and fingerprints in identity cards of EU nationals "requires a reflection and a thorough analysis".⁴⁶

FRA Opinion 3

The proposal suggests to store the facial image as well as two fingerprints of the holder of an identity card. This solution is not supported in the impact assessment, which concludes that the purpose can be achieved by limiting the compulsory storage to facial images. In case the EU legislator follows the proposal and thus departs from the findings of the Commission's impact assessment, the necessity and proportionality of processing two biometric identifiers needs to be carefully re-assessed.

The EU legislator must thoroughly assess the necessity of processing and storing two types of biometric identifiers of EU nationals in national identity cards, in case it decides to follow the Commission proposal. In addition to the elements considered by the European Commission in its impact assessment, the EU legislator should also take into account possible risks that biometric data may be unlawfully accessed, including by criminals who may use such data stored on a lost or stolen identity document to cast a fake set of fingerprints.

⁴¹ [Council Regulation \(EC\) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States](#), OJ L 385/1 (as amended).

⁴² Impact Assessment, pp. 27, 53.

⁴³ Impact Assessment, pp. 51, 60.

⁴⁴ CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013, para. 40.

⁴⁵ Also the Commission pointed out in the Impact Assessment that "ID cards serve more purposes than crossing the border" (see p. 60).

⁴⁶ European Data Protection Supervisor (2018), [EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents](#), 10 August 2018, p. 11.

4. Respecting human dignity when collecting biometric data

Article 4 of the proposal contains specific safeguards for the collection of biometric data from EU citizens and underlines that the dignity of the person must be respected in case difficulties arise.

Nonetheless, Article 4 only applies to Chapter II on national identity cards. It is not clear neither from the operative provisions of the draft regulation, nor from the Explanatory Memorandum why this safeguard provision does not apply to Chapter IV of the proposal (residence cards for family members who are not nationals of a Member State).

This asymmetry raises fundamental rights issues in light of the fact that there are no similar requirements either for the collection of biometric data in Regulation (EC) No. 1030/2002 as last amended by Regulation (EU) 2017/1954 laying down the uniform format of residence permits for third-country nationals. The format and security features specified by that regulation will be applicable to residence documents issued to third-country family members of EU citizens enjoying the right to free movement. Chapter IV of the proposal merely refers to the technical specifications under Regulation (EC) No. 1030/2002 as amended without references on how biometric identifiers should be collected and under which conditions and safeguards.

FRA Opinion 4

The safeguard to respect human dignity in case there are difficulties in collecting biometric identifiers only applies to identity cards and not to residence cards. This asymmetry is not justified.

The EU legislator should move the second paragraph of Article 4 to Chapter V which includes common provisions, so that the safeguard included therein also applies when Member States collect biometric identifiers from third-country national family members of EU citizens to issue their residence cards and permanent residence cards in the new format.

5. Collecting biometric data from children

For identity cards, fingerprints are collected from children as of the age of 12 years, according to Article 3 (5) (a) of the proposal. This provision corresponds to the age limit included in Article 1 of Regulation (EC) No. 444/2009,⁴⁷ amending the regulation on passports.⁴⁸ For facial images, no minimum age limit is introduced.

For residence cards issued to third-country national family members, the minimum age at which fingerprints are included in the chip is six years.⁴⁹

The processing of biometric data from children is particularly sensitive. Under Article 24 of the Charter, children have the right to such protection and care as is necessary for their well-being. Any processing of children's biometric data must be subject to a stricter necessity and proportionality test, compared to adults.

The reliability of the match is important to determine the age limit when collecting fingerprints of children. According to research carried out by the Joint Research Centre (JRC) of the European Commission, only the results for children between 13-17 years old are very similar to those of adults when biometrics are matched seven years later after having been collected.⁵⁰ Under Article 20 of the Free Movement Directive, the permanent residence card issued to third-country national family members will be valid for ten years and is subsequently automatically renewed. This means, that third-country national children to whom a permanent residence card is issued may find themselves in a situation where the fingerprints stored in the card when they were six years old may be used for comparisons when they are 16 years of age. In these cases, there is a non-negligible risk of a false match. In its Opinion on the revision of the Visa Information System, FRA suggested to involve a dactyloscopic expert to verify the accuracy of a match when the comparison is done with fingerprints or a facial image taken more than five years earlier.⁵¹

Fingerprints should be collected in a child-sensitive and child-friendly manner. Recital (11) of the proposal envisages that the fingerprinting procedure should take into account specific needs of children and be applied in line with specific safeguards in the Charter and other human rights instruments. However, contrary to Regulation (EC) No. 444/2009 on passports which introduced safeguards referring to the United Nations Convention on the Rights of the Child in the operative clauses (Article 1a inserted into the original EU passport regulation), the proposal confines this important child protection safeguard only to a Recital.

As per Article 4 (1) of the proposal, biometric identifiers will have to be collected by "qualified and duly authorised staff designated by the national authorities responsible for issuing identity cards". Providing appropriate training to the staff tasked with

⁴⁷ [Regulation \(EC\) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation \(EC\) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States](#), OJ L 142/1.

⁴⁸ [Council Regulation \(EC\) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States](#), OJ L 385/1.

⁴⁹ [Council Regulation \(EC\) No. 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals](#), OJ L 157/1, Art. 4b.

⁵⁰ European Commission (2018), *Automatic fingerprint recognition: from children to elderly, Ageing and age effects*, JRC technical reports, 2018, pp. 40, 43.

⁵¹ FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on the revised Visa Information System and its fundamental rights implications*, FRA Opinion – 2/2018 [VIS], Vienna, 30 August 2018, pp. 9, 36-38..

collecting biometric data reduces the risk of fundamental rights violations, for example, in situations where, for various reasons, the individual is reluctant to provide his/her fingerprints or to remove clothing for taking a facial image. Training should, therefore, not only focus on the technical aspects of capturing biometric identifiers, but also on the treatment of the persons being fingerprinted.⁵² In this context, particular attention must be paid when taking biometric data from children.

To respect the right to private life set out in Article 7 of the Charter and Article 8 of the European Convention on Human Rights, and to allow national authorities to collect biometrics as far as possible in a gender-sensitive manner, particularly in case of women and girls, sufficient female staff are needed in the national authorities responsible for issuing identity cards.

FRA Opinion 5

Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions that public authorities and private actors take in relation to children. This implies that when children's biometric data are exceptionally stored, these should not adversely affect them, including by exposing them to a heightened risk of wrong matches. Furthermore, there should be an operational clause obliging relevant authorities to collect fingerprints in a child-sensitive and gender-sensitive manner.

The EU legislator should move the content of Recital (11) to the operative part of the Regulation (for example under Chapter V on common provisions), stipulating that the collection of biometric identifiers should be undertaken in a child-sensitive and in a gender-sensitive manner.

To avoid the risk of wrong matches, the EU legislator should set the minimum age of storing fingerprints for children in residence cards for third-country national family members at 12 years – the minimum fingerprinting age set for identity cards. Alternatively, the EU legislator should require that any match concerning children carried out with biometric identifiers taken more than five years before should be subject to a compulsory manual check by a dactyloscopic expert.

6. Collecting biometric data from older persons and persons with disabilities

Persons with disabilities

Recital (13) of the proposal underlines that the regulation must respect the UN Convention on the Rights of Persons with Disabilities.⁵³ The integration of persons with disabilities is also included in Article 26 of the EU Charter. Furthermore, disability must not result in unequal treatment or discrimination prohibited by Articles 20 (equality before the law) and 21 (non-discrimination) of the Charter.

Persons applying for national identity cards will be exempted from the obligation to provide fingerprints if this is physically impossible, according to Article 3 (5) (b) of the proposal. It is also possible that the facial image cannot successfully be used for facial

⁵² See similarly, FRA (2018), [Under watchful eyes: biometrics, EU IT systems and fundamental rights](#), Luxembourg, Publications Office, March 2018, pp. 11 and 57.

⁵³ United Nations (2006), [Convention on the Rights of Persons with Disabilities](#), 13 December 2006.

image matching because of disability, an accident or paralysis, for example. This situation is, however, not covered in the proposal.

Older people

Article 25 of the Charter recognises the rights of the older people to lead a life in dignity and independence and to participate in social and cultural life. By 2080, Eurostat projects that those aged 65 years or over will account for 29.1 % of the EU-28 population, compared with 19.2 % in 2016.⁵⁴ The number of older EU citizens travelling is expected to continue to rise in the future.⁵⁵ Higher life-expectancy will likely be accompanied by a wish to participate actively in civil, political, cultural life of society.⁵⁶ This may also result in older people having to use their identity cards more frequently, for example, as they visit another EU Member State.

Under Article 3 (10) of the proposal, identity cards will have a maximum period of validity of 10 years, but derogations may be provided for specific age groups. National law may provide for facilitation for specific age groups. Several Member States issue residence documents for an indefinite or a period exceeding 10 years for older persons, as Table 1 shows.⁵⁷ Such derogations are well justified in light of Article 25 of the Charter relating to the rights of older persons.

Table 1: Validity periods of identity documents for older people in selected Member States

Member State	As of age	Validity period
Belgium	75	30
Bulgaria	58	indefinite
Czech Republic	70	35
Hungary	65	indefinite
Romania	55	indefinite
Slovakia	60	indefinite
Slovenia	70	indefinite
Spain	70	indefinite

Source: FRA, 2018 (based on Impact Assessment SWD(2018) 110 final, pp. 104-105)

However, the rationale of collecting fingerprints for older people is questionable, as fingerprint matches of older people may not be accurate.

A JRC study found that challenges exist to match fingerprints of older people, especially those above 70 years of age. The accuracy of a fingerprint match for this group is

⁵⁴ Eurostat, [People in the EU - population projections](#), as last modified on 19 June 2018, at 15:50.

⁵⁵ European Commission, [“Europe, the best destination for seniors” “Facilitating cooperation mechanisms to increase senior tourist’s travels within Europe and from third countries in the low and medium seasons”](#), Experts draft report, Annex 1, Demographic change and the rise of senior tourists. See p. 2 of the Annex: “The two indicators combined suggest that Europe shows the highest potential as source of senior travellers, due to the volume of its elderly population and the increasing penetration of travel among its population in general (by 2030, Europeans are expected to generate 89 international tourists arrivals every 100 population)” as well as figure on p. 3. The informal report was drafted upon the Commission’s request by a group of experts, see: http://ec.europa.eu/growth/sectors/tourism/offer/seniors-youth_en.

⁵⁶ See in this regard also FRA (2018), [Fundamental Rights Report 2018](#), Chapter 1, Shifting perceptions: towards a rights-based approach to ageing, Luxembourg, Publications Office, June 2018, pp. 9-31.

⁵⁷ Impact Assessment, pp. 26, 105, 106.

comparable to that of children aged 5-12 (see Chapter 5).⁵⁸ This means that with advancing age, individuals will be increasingly at risk of false matches. In its Opinion on the revision of the Visa Information System, FRA suggested to verify the accuracy of a match manually by involving dactyloscopic and/or facial image experts.⁵⁹

FRA Opinion 6

The proposal includes a reference to the rights of persons with disabilities but such reference does not mention the relevant article of the Charter. Under Article 25 of the Charter, older people have the right to lead a life in dignity and independence and to participate in social and cultural life. The life-expectancy is increasing and older people are increasingly mobile. The Regulation could better reflect this reality.

The EU legislator should reformulate Recital (13) of the proposal to read “When implementing this Regulation EU Member States should respect the obligations....” adding also a reference to Article 26 of the Charter.

To avoid the risk of wrong matches, the EU legislator should avoid compulsory storage of fingerprints of people older than 70 years. Alternatively, the EU legislator should require that any match concerning people aged 70 years or older must be subject to a compulsory manual check by a dactyloscopic and/or facial image expert.

⁵⁸ European Commission (2018), [Automatic fingerprint recognition: from children to elderly, Ageing and age effects](#), JRC technical reports, 2018, pp. 40, 61.

⁵⁹ FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on the revised Visa Information System and its fundamental rights implications*, FRA Opinion – 2/2018 [VIS], Vienna, 30 August 2018, pp. 9, 38.



Publications Office

ISBN: 978-92-9474-238-4
doi: 10.2811/560520



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](https://www.facebook.com/fundamentalrights)
■ [linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency) ■
twitter.com/EURightsAgency