FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

FRA Opinion – 6/2016
[Eurodac]

Vienna, 22 December 2016

The impact of the proposal for a revised Eurodac Regulation on fundamental rights

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 (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 previous opinions of FRA on related issues; in particular the FRA opinion concerning an EU common list of safe countries of origin,[1] and the FRA opinion concerning the proposal for a revised Dublin Regulation,[2]

Having regard to the request of the European Parliament of 6 December 2016 to FRA for an opinion "on the relevant draft provisions [of the Eurodac proposal] referring, in particular, to the extension of the Regulation's scope to anyone over 6 years, as well as the potential impact of the new system on minors (both unaccompanied or in families) [as well as …] on a possible modification of the current system facilitating the access by law enforcement authorities and Europol to Eurodac."

SUBMITS THE FOLLOWING OPINION:

---

1 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights concerning an EU common list of safe countries of origin.*

2 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on children of the proposal for a revised Dublin Regulation (COM(2016)270 final; 2016/0133 COD).*

Opinions

Dignity, liberty and physical integrity

Actions taken by European Union (EU) Member States to comply with their obligation to take fingerprints for Eurodac must respect human dignity as reflected in Article 1 of the Charter of Fundamental Rights of the European Union (the Charter) and take into account the fact that asylum seekers are in a vulnerable situation and that children are particularly vulnerable. Biometrics must be taken from children in a manner that respects human dignity and is appropriate to their age, gender and maturity.

FRA Opinion 1

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 safeguard the dignity of women and girls whose fingerprints and facial images are being taken sufficient female staff are needed.

To achieve this, Article 2 of the proposed recast Eurodac Regulation should require that biometric data are not only taken in a child-friendly and a child-sensitive manner but also in a gender-sensitive manner. Furthermore, a general safeguard underlining that fingerprints and facial images must be taken in full respect of human dignity should be inserted in Article 2 (5).

FRA Opinion 2

Asylum seekers and apprehended migrants in an irregular situation must provide fingerprints for Eurodac. As FRA pointed out in its 2015 Focus paper on '*Fundamental rights implications of the obligation to provide fingerprints for Eurodac*', compliance with this obligation should primarily be secured through effective information and counselling. This can either be provided individually and/or through outreach actions targeting migrant communities, such as focus group discussions, information sessions and similar initiatives.

Deprivation of liberty and the use of physical or psychological force to obtain fingerprints for Eurodac should be avoided because it entails a high risk of violating fundamental rights enshrined in the Charter, namely the right to human dignity (Article 1) and the right to the integrity of the person (Article 3), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4) and the right to liberty and security (Article 6). This is particularly the case for children and other vulnerable persons, such as suspected victims of torture, sexual or gender-based violence, victims of other serious crimes, or traumatised people.

An explicit prohibition to use force or resort to deprivation of liberty to take fingerprints or a facial image of children and of other vulnerable persons should be included in Article 2 of the proposed recast Eurodac Regulation. In addition, the wording "except in duly justified circumstances that are permitted under national law" should be deleted from the proposed Recital (30). Finally, a reference to FRA's 2015 Checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac (available on FRA's website) could be considered in Recital (30).

Rights of the child

Incorporating a core principle enshrined in Article 3 of the United Nations (UN) Convention on the Rights of the Child, Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions taken in relation to children by public authorities and private actors. The European Court of Human Rights (ECtHR) repeatedly underlined the extreme vulnerability of children seeking asylum or who are in an irregular situation, whether unaccompanied or accompanied by parents. The proposed recast of the Eurodac Regulation suggests reducing the age of persons to be processed in Eurodac from 14 to six years. This has several implications that must be considered.

FRA Opinion 3

The proposed recast of the Eurodac Regulation contains important safeguards regarding information to be given to children. These could, however, be further enhanced by spelling out a duty in Article 2 (2) of the proposed recast Eurodac Regulation to provide age-appropriate information to unaccompanied children also orally.

To facilitate an effective implementation of the safeguards included in the proposed recast Eurodac Regulation, the European Commission and relevant EU agencies could consider documenting and disseminating promising practices, for example, on the role of the guardian in supporting the provision of information.

FRA Opinion 4

The proposed recast Eurodac Regulation suggests processing of children's biometric data as young as six years of age to achieve the purposes set out in its Article 1, namely: applying the Dublin system, combating irregular immigration and fighting serious crime. To comply with Article 7 (respect for private and family life), Article 8 (protection of personal data) and Article 24 (the rights of the child) of the Charter, this measure can only be justified if it expressly pursues a child protection objective. More specifically, it should serve to protect child victims of trafficking and support the identification and protection of unaccompanied children who go missing, disappear or abscond, as the European Commission highlighted in its explanatory memorandum accompanying the proposed recast Eurodac Regulation. Therefore, the following changes to EU law should be made:

- ***An additional purpose to protect child victims of trafficking in human beings and to identify and protect missing children should be added to Article 1 (as Article 1 (1) (d)). Only national law enforcement authorities responsible for the prevention, detection and investigation of child trafficking as well as Europol should be able to access Eurodac to protect child victims of trafficking in human beings. The question whether general law enforcement access under Article 1 (1) (c) to Eurodac for children under the age of 14 years is proportionate, should be assessed based on additional evidence of the relevance of these data for combating terrorism and other serious crime.***
- ***Personal data stored on children under the age of 14 years should be blocked for the purposes set out in Article 1 (1) (b).***
- ***Should additional alphanumeric data of applicants for international protection be included in the future version of Eurodac, consideration should be given to record also family links (including between separated children and an accompanying adult), so as to increase the system's potential to trace and reunite missed family members and justify the use of personal data stored on children under the age of 14 years for the purpose set out in Article 1 (1) (a).***

- *An explicit duty should be included in EU law obliging Member States to record all children (under the age of 18 years) who have disappeared from reception facilities as missing persons in the Schengen Information System II (SIS II). As soon as a child is entered in SIS II as missing, his or her fingerprints and other personal data stored in Eurodac relevant for tracing missing children should, if feasible, become visible by consulting SIS II, without the need for authorities responsible for tracing missing children to access Eurodac.*
- *A rule should be included in EU law, based, for example, on Article 81 (3) of the Treaty on the Functioning of the EU (TFEU), to oblige Member State authorities which identify a missing child to contact competent national child protection authorities to undertake a needs assessment with a view to find a durable solution for the child in line with his or her best interests.*

FRA Opinion 5

To respect the duty to give a primary consideration to the best interests of the child, fingerprints should not be compared anymore with those taken in the past if the likelihood of a wrong match increases. In case of young children, the reliability of matches of fingerprints after more than five years have passed is not yet proven.

To avoid the negative consequences of a possible mismatch after a certain period has elapsed, fingerprints of children younger than 14 years should only be automatically compared for a maximum of five years. Following this period, dactyloscopic experts should only carry out manually such comparisons to avoid disadvantages for the child.

Rolled fingerprints are of higher quality compared to plain fingerprints. Given the criminal law connotation of rolled fingerprints, however, the legislator should define the type of fingerprints to enrol in Eurodac.

FRA Opinion 6

The comparison of facial images in Eurodac should only be used as an additional feature when determining the identity of a person. This is particularly important for children. A comprehensive assessment of how the processing of facial images affects a person's fundamental rights should include a review of the reliability over time of facial images of younger children. It should also consider possibly harmful practices persons may resort to in order to avoid that their facial image or the image of their children be successfully taken.

Following a hit after having simultaneously compared fingerprints and facial image, in accordance with Article 15, both biometric identifiers should always be subject to checks and verifications. The EU legislator should consider making this explicit in Article 26 (4) and Recital 31, which would minimise any risks for false matches.

The EU legislator should consider amending Article 42 (4) of the proposed recast Eurodac Regulation and make recommendations for the introduction of facial recognition technology subject to a comprehensive evaluation of the impact the processing of facial images has on fundamental rights. FRA would be ready to support such an evaluation.

FRA Opinion 7

To evaluate better the impact of the Eurodac Regulation on children, monthly statistics provided by eu-LISA under Article 9 of the proposal should be broken down by age and sex to understand how many boys and girls under the age of 18 years are affected. Children's statistics concerning the reliability of biometric matching should be broken down by year of birth.

The right to asylum

Article 18 of the Charter guarantees the right to asylum. The proposed amendments to the Eurodac Regulation affect this right in different ways. Although the changes affect all asylum applicants, its consequences increase in case of children.

FRA Opinion 8

When personal data processed in Eurodac are shared with third countries, sufficient safeguards must be in place. Such safeguards are required to avoid exposing applicants for international protection and their families to risks of serious harm by actors in the country of origin, as well as to comply with the right to protection of personal data enshrined in Article 8 of the Charter. For this purpose, the following measures should be considered:

- ***Article 38 (1) of the proposed recast Eurodac Regulation should be amended to exclude sharing personal data of asylum applicants with their country of origin to prepare their return as long as no final decision has been taken on the application for international protection;***
- ***Article 37 (2) contains an important fundamental rights safeguard that should also apply to personal data stored in Eurodac and not only to data exchanged between Member States.***

Personal data that can be transferred to third countries should be expressly listed in Article 38. Data that are not needed for the purpose of return, such as the unique identification number or data on Dublin transfers should be excluded from the list of transferable data.

When the transfer of personal data to third countries concerns applicants for international protection, the EU legislator could require Member States to document the transfer and its justification, and make such documentation available to the data protection supervisory authority on request, similarly to what is envisaged in Article 37 (3) of the new Data Protection Directive.

FRA Opinion 9

Eurodac needs to be immunised against unlawful access to personal data of applicants for international protection. Abusive access to personal data stored in Eurodac by the country of origin would undermine the right to asylum enshrined in Article 18 of the Charter. It may also expose family members, including children, who remained in the country of origin to acts of retaliation to force dissidents to come back home or enable the kidnapping of applicants for international protection.

The EU legislator should carefully assess the necessity and proportionality of centrally storing the name, surname, nationality, date and place of birth, as well as information on the travel document of an applicant for international protection for a period as long as 10 years. To reduce risk of abuse, the EU legislator should consider blocking the personal

data of international protection applicants listed in Article 13 (2) (c)-(e) and (h) of the proposal until the international protection claim is rejected in the final instance that these are not automatically visible in case of a Eurodac match. Where such data are needed to achieve the objectives laid down in Article 1 (1) (a) and (c) of the proposed recast Eurodac Regulation, it should be exchanged bilaterally between Member States as it is currently the case under Regulation (EU) No. 603/2013.

FRA Opinion 10

The provisions in Articles 15 (4) and 16 (5) of the proposed recast Eurodac Regulation which deal with the way to handle cases of multiple matches could be interpreted in different ways.

For the sake of normative clarity and enhanced coherence between connected legislative instruments, these provisions should be rephrased, in line with the explanatory memorandum to the proposed recast Eurodac Regulation. The EU legislator should make it explicit that the new rule ('hierarchy of Eurodac hits') reflects without prejudice to the hierarchy of criteria as laid down in the Dublin Regulation.

Respect for private life, data protection and access to justice

The proposed changes to the Eurodac Regulation lowering the age of persons recorded in the system from 14 to six years, storing additional alphanumeric data and expanding the purpose to include the fight against irregular migration may lead to disproportionate consequences for children and increase the amount of data available to law enforcement. Additional changes concerning access by law enforcement are being discussed.

FRA Opinion 11

The new purpose of Eurodac to "assist with the control of illegal immigration [...] and secondary movements" must be seen in light of other existing and planned information technology (IT)-systems that also pursue such objectives. Used together with other IT-systems, the broad definition of this purpose may result in a disproportionate negative impact on children.

It would therefore be advisable to formulate Article 1 (1) (b) of the proposed recast Eurodac Regulation in stricter terms by deleting the following part of the sentence "with the control of illegal immigration to and secondary movements within the Union and".

Moreover, it would be advisable to replace the term illegal immigration with "irregular immigration" throughout the proposed recast Eurodac Regulation.

FRA Opinion 12

In many cases, asylum seekers who enter the EU in an irregular manner are first fingerprinted as irregular border crossers. When they formally lodge a claim for international protection, they are fingerprinted again as applicants for international protection. Double fingerprinting could lead to an excessive interference into the right to respect for private life enshrined in Article 7 of the Charter and Article 8 of the European Convention on Human Rights (ECHR). It could also create situations of tensions leading to the use of coercive measures to enforce fingerprinting.

To avoid having two separate entries of the same person, consideration could be given to allow the recording of persons apprehended in connection with their irregular crossing of the external border who express the wish to apply for asylum ("make" an application) as

applicants for international protection, even when under national law the application is formally lodged only subsequently. This would also help to ensure that an asylum request is visible in the system from the beginning, which can increase protection from **refoulement.**

FRA Opinion 13

Eurodac registrations may often be carried out under time pressure in situations of stress. Newly arrived asylum seekers and migrants may not yet trust the authorities and, therefore, may provide incorrect personal data. This is likely to lead to a significant amount of incorrect personal data being stored in Eurodac, particularly as alphanumeric data will also be stored.

To reduce the negative impact of mistakes contained in Eurodac, a duty to review the accuracy of data stored and to rectify possible mistakes could be inserted in Article 28 of the proposed recast Eurodac Regulation, for example, when issuing a residence permit or a return decision to the third-country national.

FRA Opinion 14

The principle of proportionality enshrined in Article 52 (1) of the Charter, as interpreted by the Court of Justice of the EU, requires that access to personal data for law enforcement purposes is subject to adequate safeguards and that the retention of the data reflects its law enforcement relevance.

Information contained in Eurodac is collected without any evidence suggesting a link to terrorism or other serious crime, and pertains to a significant extent to persons in a vulnerable situation. In the absence of the assessment envisaged under Article 40 of Eurodac Regulation (EU) No. 603/2013, the key principles of the current model of law enforcement access to Eurodac reflected in Articles 21 and 22 of the proposed recast – in particular the clear purpose limitation and the hit/no hit access based on biometric features only – need to remain in place for access of Member States' law enforcement agencies as well as Europol.

Differentiation between the periods for which law enforcement access is possible should take into account the nature of the data and reflect the vulnerable situation of applicants for international protection, in particular the need to avoid that sensitive data are transferred to third countries. Possible future mechanisms to facilitate the interoperability of EU large-scale IT-systems should take into account the need to retain the safeguards specific for each system.

Introduction

In light of the request by the European Parliament, this opinion by the European Union Agency for Fundamental Rights (FRA) analyses the effects on children of the proposed recast Eurodac Regulation, which suggests to process personal data of children as of six years of age. As requested, it also analyses possible modifications relating to law enforcement access to Eurodac. It does not look at all fundamental rights issues arising from the proposed changes to the Eurodac Regulation.

The opinion touches in particular on the following fundamental rights of the Charter of Fundamental Rights of the European Union (Charter):

- the right to human dignity (Article 1)
- the right to the integrity of the person (Article 3)
- the prohibition of torture and inhuman or degrading treatment or punishment (Article 4)
- the right to respect for private and family life (Article 7)
- the right to the protection of personal data (Article 8)
- the right to asylum (Article 18)
- the protection in the event of removal, expulsion or extradition (Article 19)
- the protection of the rights of the child (Article 24)
- the right to an effective remedy and to fair trial (Article 47).

This opinion complements the opinion of the European Data Protection Supervisor on the first reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations), Opinion 7/2016, submitted on 21 September 2016.

Eurodac

Eurodac, which stands for European Dactyloscopy, is a large-scale IT-system that stores fingerprints. It has been set up to help determine the Member State responsible to examine an application for international protection based on the criteria set out in the Dublin Regulation (Regulation (EU) No. 604/2013).[3] The European Agency for the operational management of large-scale IT-systems in the area of freedom, security and justice, eu-LISA, manages Eurodac. The Eurodac Regulation applies to all EU Member States as well as to the Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland), although Ireland is only bound by its 2000 version.[4]

Eurodac is one of the three existing large-scale IT-systems created at EU level in the field of justice and home affairs. The other two are the Visa Information System (VIS)[5] to manage visa applications and the second generation Schengen Information System (SIS II) which

---

3 Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 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, OJ L 180, 29.6.2013, pp. 31-59.

4 Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, pp. 1-10.

5 Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), 9 July 2008, OJ L 218, 13.8.2008, pp. 60-81.

contains alerts on persons and objects (e.g. missing persons or stolen cars; entry bans).[6] In 2014 Eurodac contained the fingerprints of nearly 2,7 million persons.[7] In the near future, two more databases, namely the Entry-Exit-System (EES) and the European Travel Information and Authorisation System (ETIAS) will be set up. EES will record border crossings by third-country nationals who are entitled to visit the Schengen area without a visa.[8] ETIAS will gather data on visa-exempt third-country nationals prior to their arrival at the border to determine whether or not the person could enter the EU.

Figure 1: Current and planned large scale IT-systems in the EU and categories of persons covered

Eurodac	Applicants for international protection and persons who have been apprehended for irregular entry or *irregular stay* in an EU Member State
SIS II	Persons or objects related to criminal offences, missing persons, third-country nationals with entry bans, *and return decisions*
VIS	Third-country nationals who have applied for short-stay visas
EES	*Third-country nationals visiting the Schengen area for a short stay (max. 90 days in any period of 180 days)*
ETIAS	*Visa-exempt third-country nationals*

Note: Proposed systems and proposed changes in italics.

Source: FRA (2016)

Eurodac was initially established in 2000[9] and subsequently revised in 2013 by Regulation (EU) No. 603/2013.[10] Under the current system, all asylum seekers and migrants

---

6 Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, pp. 4–23.

7 eu-Lisa (2015). *Annual report on the 2014 activities of the Central System of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000*, p. 11, https://ico.org.uk/media/about-the-ico/documents/1432237/eurodac-2014-annual-report.pdf.

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

9 Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, pp. 1-10.

10 Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013, pp. 1-30.

apprehended in connection with an irregular border crossing – except for children under the age of 14 years – must provide their fingerprints, which are stored in Eurodac. This allows a Member State to know if the individual has already applied for asylum elsewhere or whether he or she has been apprehended in another Member State after an irregular entry. On the basis of this information, a Member State can determine whether or not it is responsible to examine an application for international protection under the rules established in the Dublin Regulation.[11] The 2013 amendments also introduced the possibility for national law enforcement authorities and Europol to access data for the prevention, detection or investigation of terrorist offences or of other serious criminal offences but due to practical obstacles Europol has not yet been able to access Eurodac.

The proposed changes to the Eurodac Regulation are significant from a fundamental rights point of view. They can be grouped in three categories. First, as illustrated in Figure 1, the proposal suggests to expand the purpose of Eurodac so that it can also be used to control irregular immigration and secondary movements within the Union. The proposal will establish a duty to store personal (including biometric) data of apprehended migrants who are in an irregular situation.[12] Currently, under Article 17 (c) of Regulation (EU) No. 603/2013, Member States can only *compare* fingerprints of apprehended migrants in an irregular situation with those stored in Eurodac, in order to establish their identity (which is necessary for return purposes).

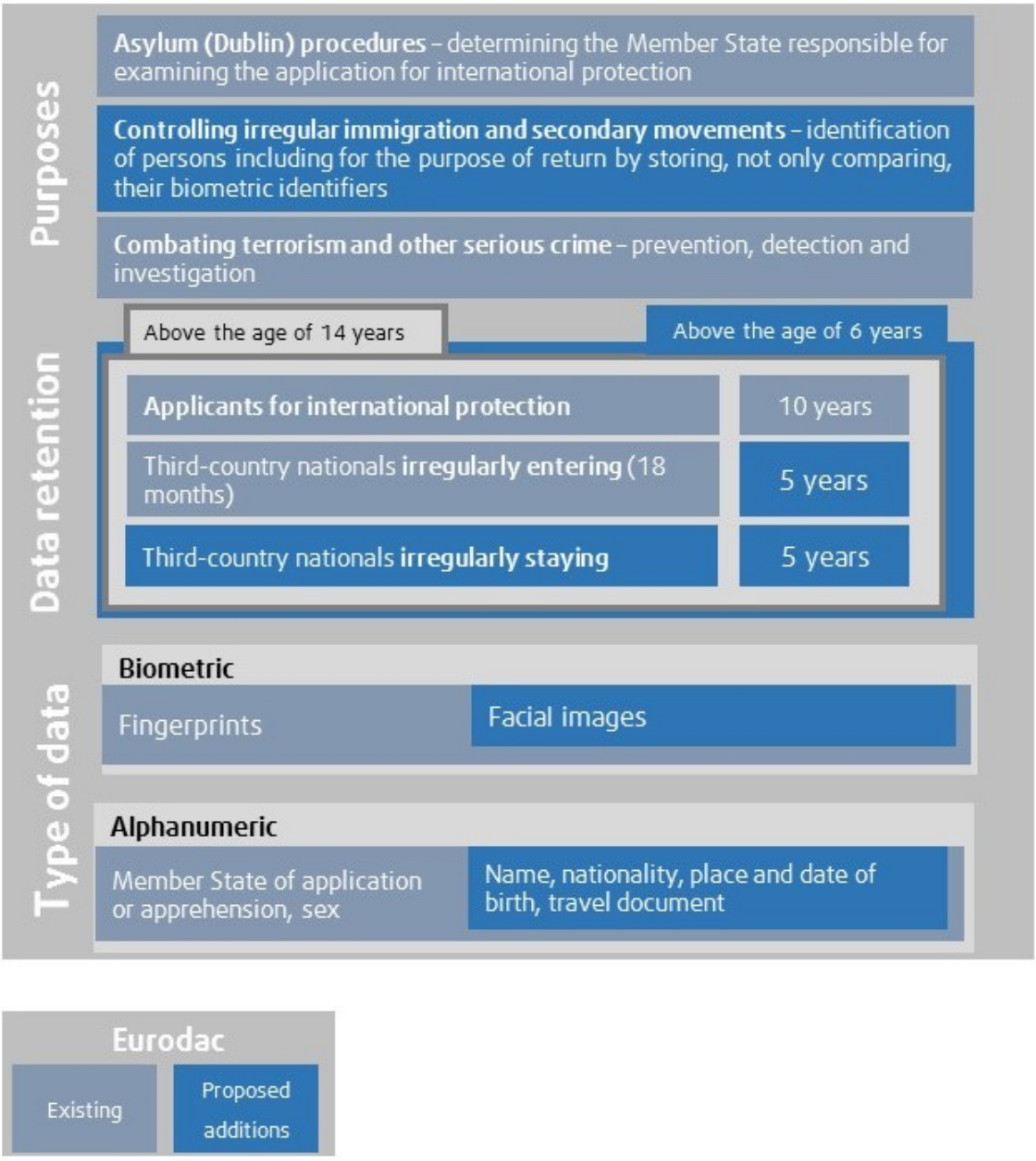
A second important set of changes concern the retention of personal data – which will be increased to five years for persons who do not apply for international protection – and the processing of biometric data from persons as of six years of age.

The third group of changes relate to the type of data processed. The proposal suggests to process two types of biometric data (fingerprints and facial images). In addition, the personal data to be stored in the central system – which currently is essentially a database of fingerprints – should be substantially expanded to include also name, nationality, place and date of birth, and travel document details.

---

[11] Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 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, OJ L 180, 29.6.2013, pp. 31-59.
European Commission, *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)*, Brussels, 4 May 2016, COM(2016) 272 final, Article 1 (1) (b).

Figure 2: Key features of Eurodac and the proposed changes



Source: FRA (2016), based on EU (proposed) legislation

The following four sections will examine how these and other changes affect children, including the implications of these and possible other changes on the access to Eurodac for law enforcement purposes.

1. Dignity, liberty and physical integrity

Registration is a fundamental component of international refugee protection. It helps protect refugees against *refoulement*, arbitrary arrest and detention, is necessary to give access to services, and enables the identification of vulnerable people.[13] Systematic registration also helps address the host society's security concerns. Under EU law, registration includes the taking of biometric data, currently fingerprints.

Actions taken by EU Member States to enforce their obligation to take fingerprints for Eurodac must respect human dignity in line with Article 1 of the Charter and take into account the fact that asylum seekers are in a vulnerable situation and children seeking asylum or in an irregular situation are particularly vulnerable.

Actions to enforce the duty to collect biometric data may interfere with a number of fundamental rights guaranteed by the Charter. Interferences may involve absolute rights – such as the prohibition of torture, and other inhuman or degrading treatment of punishment – from which no derogations are possible. It may also involve rights that under certain conditions can be limited, such as the right to liberty (Article 6 of the Charter and Article 5 of the ECHR) or the right to respect for private life and the protection of personal data (Articles 7 and 8 of the Charter and in Article 8 of the ECHR). For interferences with such rights to be justified, they have to respect the requirements of the Charter and the ECHR.

This section deals with the provisions included in Article 2 of the proposal relating to the obligation to take fingerprints and a facial image. It first deals with the respect of human dignity more generally, and then discusses the use of force as well as deprivation of liberty to obtain biometric data.

1.1. Taking fingerprints in a child and gender sensitive manner

Fingerprints and facial images must be taken in full respect of human dignity in a manner which is appropriate to the child's age and maturity. This may be challenging when taking biometric data from children as young as six years of age.

If there is doubt about the age of an asylum seeking child, Member States may conduct age assessments to determine if a child is under or above six years of age, an exercise which has to be carried out in full respect of the child's dignity and which may raise additional fundamental rights challenges.

To limit possible conflicts with the UN Convention on the Rights of the Child and the rights of the child embodied in Article 24 of the Charter, Article 2 (2) of the proposed recast Eurodac Regulation requires that fingerprints and facial images be taken in a child-friendly and child-sensitive manner by officials who have been specifically trained to collect biometric data from children.

This proposed amendment will contribute significantly to reduce the risk of disrespectful treatment when collecting fingerprints. It will, however, not necessarily address one of the challenges identified by FRA in the hotspots, namely the need for gender-sensitive procedures.[14]

---

[13] UNHCR (2003), *UNHCR Handbook for Registration*, September 2003, pp. 6–7; UNHCR, *Better protecting refugees in the EU and globally*, December 2016, Section 3.

[14] FRA, *Opinion of the European Union Agency for Fundamental Rights on fundamental rights in the 'hotspots' set up in Greece and Italy*, 29 November 2016, pp. 42-43.

Procedures involving potential dignity and privacy issues vis-à-vis women should whenever possible be conducted by female staff.[15] However, FRA has observed that fingerprinting teams are often composed only or mainly of male officers. In its opinion on the hotspots, FRA has stressed the importance of having sufficient numbers of female staff for procedures that involve physical contact, such as fingerprinting for Eurodac.[16]

FRA Opinion 1

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 safeguard the dignity of women and girls whose fingerprints and facial images are being taken sufficient female staff are needed.

To achieve this, Article 2 of the proposed recast Eurodac Regulation should require that biometric data are not only taken in a child-friendly and a child-sensitive manner but also in a gender-sensitive manner. Furthermore, a general safeguard underlining that fingerprints and facial images must be taken in full respect of human dignity should be inserted in Article 2 (5).

1.2. Avoiding disproportionate sanctions

Cases of asylum seekers using acid, glue or other means to destroy their fingerprints or harming themselves to avoid registration in Eurodac have been known for several years.[17] The lack of registration in Eurodac at points of entry has gained increased attention in 2014 and 2015.[18] In some cases, this resulted from the limited capacity of front-line states to deal with increased arrivals, an issue which has meanwhile been addressed. In others, those arriving – including individuals from Eritrea, Sudan, or Syria likely in need of international protection – refused to give their fingerprints for Eurodac or to apply for asylum altogether in the first EU Member State they reached. Also these instances diminished when relocation became available for Eritreans and Syrians.

In recent years, the feasibility and appropriateness of using coercive measures to force third-country nationals to give their fingerprints has been considered. The European Agenda for Migration, stresses the importance of fully implementing the rules on taking fingerprints at the

---

[15] See for example European Parliament (2016), Report of 10 February 2016 on the situation of women refugees and asylum seekers in the EU (2015/2325(INI)) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0024+0+DOC+XML+V0//EN, or UN women (2016), Gender Assessment of the Refugee and Migration Crisis in Serbia and FYR Macedonia, www2.unwomen.org/~/media/field%20office%20eca/attachments/publications/country/serbia/gender%20assessment%20of%20the%20refugee%20and%20migration%20crisis%20in%20serbia.pdf?v=1&d=20160112T163308.

[16] FRA, *Opinion of the European Union Agency for Fundamental Rights on fundamental rights in the 'hotspots' set up in Greece and Italy*, 29 November 2016, pp. 38-39.

[17] See, for example, J. Feng, A.K. Jain, A. Ross, *Fingerprint Alteration,* MSU Technical Report, December 2009, available at: http://www.cse.msu.edu/~rossarun/pubs/FengJainRoss_AlteredFingerprint_TechReport09.pdf.

[18] See European Migration Network (EMN) (2014), *Ad-hoc query on Eurodac fingerprinting*, 22 September 2014; General Secretariat of the Council of the European Union, Meeting document to Delegations, *Best practices for upholding the obligation in the Eurodac Regulation to take fingerprints*, DS 1491/14, 30 October 2014.

borders.[19] The European Commission issued a guidance paper on how to implement the duty to take fingerprints, which also envisages as a last resort the use of coercive measures.[20]

The proposed recast Eurodac Regulation reflects these concerns strengthening the obligation to provide fingerprints and a facial image. If adopted, it will allow states to impose administrative sanctions in case of non-compliance. According to proposed Article 2 (3) such sanctions must be effective, proportionate and dissuasive. Read together with proposed recital (30) possible steps that Member States may take are deprivation of liberty, the use of force (as a last resort) to take fingerprints or a facial image, and the processing of an application for international protection in an accelerated manner as per Article 31 (8) (i) of the Asylum Procedures Directive.[21]

Article 2 (4) of the proposal contains a safeguard to avoid that sanctions are imposed when taking biometric data is not possible due to the conditions of the fingerprints or face, although this safeguard – which should logically apply to everyone – is limited to children and vulnerable people. Furthermore, if a child refuses to give his/her fingerprint or facial image, and "there are reasonable grounds to suspect that there are child safeguarding or protection risks", the child must be referred to protection systems. Proposed recital (30) also notes that vulnerable persons and children "should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law".

There may be different reasons why people may not feel comfortable in giving fingerprints. A desire to reach the European country of their choice without the risk of being sent back to a Member State of transit under the Dublin system is presumably the main reason for refusing to give fingerprints, but there may be other explanations. It is possible that asylum seekers have had bad experiences with giving fingerprints to the police in their country of origin, or that they fear the fingerprints may be shared with the country of origin, which could endanger family members. Other people may hesitate to give their fingerprints because they are generally afraid of technology or may not trust – in light of global surveillance revelations, for example – that the collected data will be handled in conformity with data protection principles.

The right to protection of personal data as laid down in Article 8 of the Charter and Article 16 of the TFEU requires fair processing, which includes adequately informing persons whose fingerprints are taken. This means that, before resorting to sanctions or coercive measures, asylum seekers and migrants in an irregular situation need to be provided with an effective opportunity to comply with the duty to provide fingerprints. They must be fully informed of all their options, the rationale for collecting fingerprints, the manner in which fingerprints will be processed, and the consequences of not giving their fingerprints.

To support officers working on the ground, in 2015, FRA produced a checklist in response to instances of alleged excessive use of force brought to FRA's attention from Italy.[22] FRA pointed

---

[19] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Agenda for Migration*, COM(2015) 240 final, 13 May 2015.

[20] European Commission, *Implementation of the Eurodac Regulation as regards the obligation to take fingerprints*, Commission Staff Working Document, SWD(2015) 150 final, 27 May 2015.

[21] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013) on common procedures for granting and withdrawing international protection (recast), OJ L 180, 29/06/2013, pp. 60–95.

[22] FRA (2015), *Fundamental rights implications of the obligation to provide fingerprints for Eurodac,* Luxembourg, Publications Office. The publication contains a checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac. Excessive use of force to take fingerprints has been also

out that compliance with the obligation to take fingerprints should primarily be secured through effective information and counselling, carried out individually as well as through outreach actions targeting migrant communities, such as focus group discussions, information sessions and similar initiatives. Respecting the principle of proportionality – which is a general principle of EU law[23] – requires the use of less invasive means, whenever possible.

Concerning the use of force to take fingerprints, FRA has already pointed out in the past that given the vulnerability of the people concerned and the obligation to use the least invasive means, it is difficult to imagine a situation in which using force to obtain fingerprints for Eurodac would be justified.[24] In specific circumstances it may meet the threshold of torture, or other inhuman or degrading treatment or punishment prohibited by Article 4 of the Charter and Article 3 of the ECHR. Such prohibition is absolute, meaning that any use of force that reaches the threshold prohibited by Article 3 of the ECHR will always be unlawful. Use of force that does not meet this threshold can still raise fundamental rights concerns, particularly in light of Article 3 of the Charter, which enshrines the right of everyone to respect his or her physical and mental integrity. When force is used to compel a person to do something, the circumstances of each individual case must be assessed to determine whether the use of force was necessary and proportionate, and would thus still constitute a lawful interference in light of the standards set forth in Article 52 (1) of the Charter. Given their heightened vulnerability, it can be assumed that use of force will never be justified in case of children.

As regards deprivation of liberty, Article 6 of the Charter and Article 5 of the ECHR stipulate the right to liberty, with the latter listing a set of permissible grounds for detention. These grounds include non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law (Article 5 (1) (b)) and the prevention of unauthorised entry and detention for the purpose of removal (Article 5 (1) (f)). Proposed Article 2 (3) will allow detention as a means of last resort "to determine or verify a third-country national's identity", mirroring Article 8 (3) (a) of the Reception Conditions Directive (2013/33/EU).[25] Given that the fingerprints or the facial image can only serve to verify identity in case a person is already registered in Eurodac, this provision would exclude detention of persons apprehended in connection with the irregular crossing of the external border. As their data would normally not be stored in the IT-system, the fingerprints, once taken, will not help with identification. In such cases, detention would only be justified on the basis of Article 5 (1) (b) of the ECHR to secure the fulfilment of an obligation prescribed by law. In such cases, detention must comply with the requirements the European Court of Human Rights (ECtHR) established: the possibility of deprivation of liberty must be provided for under national law; it must be aimed only at fulfilment of the obligation to provide

---

subject of an Amnesty International report published in November 2016, which is not limited to hotspots. See Amnesty International (2016), *Hotspot Italy: How EU's flagship approach leads to violations of refugee and migrant rights*, 3 November 2016.

[23] See e.g. CJEU, C-413/99, *Baumbast*, 17 September 2002, paras. 90-94; CJEU, C-200/02, *Catherine Chen v. Secretary of State*, 19 October 2004, para. 32; CJEU, C-41/02, *Commission v. Netherlands (Vitamins drops)*, 2 December 2004, para. 46, and CJEU, C-343/09, *Afton Chemical v. Secretary of State for Transport*, 8 July 2010, para. 45. For more on the principle of proportionality as a general principle of EU law, consider e.g. Hofmann, H.C.H., 'General Principles of EU law and EU administrative law' in *European Union Law* (Barnard, C., Peers, S., eds.), Oxford, OUP, 2014.

[24] FRA (2015), *Fundamental rights implications of the obligation to provide fingerprints for Eurodac,* Luxembourg, Publications Office, pp. 8-9.

[25] Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection, OJ L 180, 29.6.2013, pp. 96–116.

fingerprints; it must not be punitive, should be of limited duration, and cease the moment the obligation is fulfilled.[26] Moreover, a balance must be struck between the importance in a democratic society of securing the immediate fulfilment of the obligation in question, and the importance of the right to liberty. The duration of detention is also a relevant factor in drawing such a balance.[27] An individual must also be duly informed of the detention order.[28]

According to Article 37 of the UN Convention on the Rights of the Child, children may be deprived of liberty "only as a measure of last resort and for the shortest appropriate period of time". Regardless of the ground for detention, when interpreting Article 5 of the ECHR, the ECtHR held that the detention of children (whether accompanied by their parents or not) is arbitrary in facilities which are inadequate to cater for their specific needs.[29] In light of human rights law development against immigration detention of children it is difficult to justify deprivation of liberty of a child to coerce him or her to give fingerprints or to take his/her facial image.[30]

Children, suspected victims of torture, sexual or gender-based violence, victims of other serious crimes, as well as traumatised people should not be coerced into giving fingerprints, nor should other people usually considered to be vulnerable.

FRA Opinion 2

Asylum seekers and apprehended migrants in an irregular situation must provide fingerprints for Eurodac. As FRA pointed out in its 2015 Focus paper on '*Fundamental rights implications of the obligation to provide fingerprints for Eurodac*', compliance with this obligation should primarily be secured through effective information and counselling. This can either be provided individually and/or through outreach actions targeting migrant communities, such as focus group discussions, information sessions and similar initiatives.

Deprivation of liberty and the use of physical or psychological force to obtain fingerprints for Eurodac should be avoided because it entails a high risk of violating fundamental rights enshrined in the Charter, namely the right to human dignity (Article 1) and the right to the integrity of the person (Article 3), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4) and the right to liberty and security (Article 6). This is particularly the

---

[26] ECtHR, *Göthlin v. Sweden*, No. 8307/11, 16 October 2014, para. 57.; and *Vasileva v. Denmark*, No. 52792/99, 25 September 2003, para. 36.

[27] ECtHR, *Vasileva v. Denmark*, No. 52792/99, 25 September 2003, para. 37 and *Göthlin v. Sweden*, No. 8307/11, 16 October 2014, para 58.

[28] ECtHR, *Petukhova v. Russia*, No. 28796/07, 2 May2013, paras. 58–59.

[29] ECtHR, *A.B. and Others v. France*, No. 11593/12, 12 July 2016; ECtHR, *R.M. and M.M. v. France*, No. 33201/11, 12 July 2016; ECtHR, *A.M. and Others v. France*, No. 24587/12, 12 July 2016; ECtHR, *R.K. v. France*, No. 68264/14, 12 July 2016; ECtHR, *R.C. v. France*, No. 76491/14, 12 July 2016; ECtHR, *Popov v. France*, Nos. 39472/07 and 39474/07, 19 January 2012, paras. 118-120; ECtHR, *Muskhadzhiyeva and Others v. Belgium*, No. 41442/07, 19 January 2010, paras. 74-75; ECtHR, *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, No. 13178/03, 12 October 2006, paras. 100-102.

[30] See, for example: European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (2009), *20 years of combating torture. 19th General Report of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT)*, Strasbourg, Council of Europe, para. 97; Inter-American Court of Human Rights, *Rights and guarantees of children in the context of migration and/or in need of international protection,* Advisory Opinion OC-21/14 of 19 August 2014, para. 160; Council of Europe, Parliamentary Assembly, Resolution 2020 (2014) on the alternatives to immigration detention of children, para. 9 (1) and Recommendation 2056 (2014) on the alternatives to immigration detention of children, para. 2.

case for children and other vulnerable persons, such as suspected victims of torture, sexual or gender-based violence, victims of other serious crimes, or traumatised people.

An explicit prohibition to use force or resort to deprivation of liberty to take fingerprints or a facial image of children and of other vulnerable persons should be included in Article 2 of the proposed recast Eurodac Regulation. In addition, the wording "except in duly justified circumstances that are permitted under national law" should be deleted from the proposed Recital (30). Finally, a reference to FRA's 2015 Checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac (available on FRA's website) could be considered in Recital (30).

2. Rights of the child

The ECtHR repeatedly underlined the extreme vulnerability of children seeking asylum or in an irregular situation, whether unaccompanied or accompanied by parents.[31] Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions taken in relation to children by public authorities and private actors. In this regard, Member States must provide to the child such protection and care as is necessary for the child's well-being and development. According to Article 3 of the UN Convention on the Rights of the Child, they should also ensure that institutions, services and facilities responsible for the care or protection of children promote and safeguard the child's best interests and wellbeing. The principle of the best interests of the child as a primary consideration is reiterated in recital (26) of the proposed recast Eurodac Regulation.

This section examines different aspects of the proposed changes that relate directly to children. It first deals with the need to provide effective information on Eurodac to children in a manner which they can understand. It then examines the possible impact of collecting biometric data from children as of six years of age. Biometric data are a special category of personal data. Processing of biometric data could create significant risks to the individual's fundamental rights and freedoms.[32] It therefore merits specific safeguards. The sensitivity of such biometric data increases further when it concerns children, also because the retention of their data may affect their lives although they did not participate in the parents' decision to migrate. The proposed recast Eurodac Regulation envisages two important changes in this regard: the processing of biometric data for children aged six years and above and the processing of facial images. Sections 2.2 deals with the new age limit in Eurodac, 2.3 with fingerprints and 2.4 with facial images; Section 2.5 ends with suggestions to break down regular statistics by age.

2.1. Effectively informing unaccompanied children

The right to be informed on the processing of one's personal data is a pre-condition for the exercise of other rights related to the protection of personal data guaranteed under Article 16 TFEU and Article 8 of the Charter. It includes the right to information on the identity of the data controller, the purpose of the processing, the recipients of the data, and the right to access to own data and to have it rectified.[33] The General Data Protection Regulation (Regulation (EU) 2016/679), which will apply from May 2018, contains a broader list, including information on the retention period or the criteria for establishing it.[34] It also requires that such information is provided in a "concise, transparent, intelligible and easily

---

[31] See ECtHR, *Tarakhel v. Switzerland*, No. 29217/12, 4 November 2014, para. 99. ECtHR, *Popov v. France*, Nos. 39472/07 and 39474/07, 19 January 2012, para. 91. ECtHR, *Rahimi v. Greece*, No. 8687/08, 5 July 2011, para. 87; *Abdullahi Elmi and Aweys Abubakar v. Malta*, Nos. 25794/13 and 28151/13, 22 November 2016, para. 113.

[32] 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), recital (51) and Article 9.

[33] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50, Article 10.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88, Art. 13.

accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[35] The information should be provided in writing but other appropriate forms are possible, including orally where requested by the data subject.

Coercive measures to enforce registration should never be used against children – as pointed out in Section 1. It is, therefore, essential that information is not only provided to the data subjects, but that it is also understood by them and their parents or caretakers.

As illustrated by interviews carried out by FRA for its project on biometrics,[36] the purpose of the fingerprinting is not always clearly understood. With regard to unaccompanied children, it would be important to clearly explain the purpose of the fingerprinting and how it impacts on the Dublin rules. The proposed changes to the Dublin Regulation (2016) state that only if an unaccompanied child is fingerprinted as an applicant for international protection are the rules on Member State responsibility for examining the claim affected. Fingerprinting for other purposes does not affect the Dublin rules. To improve the willingness to be fingerprinted this should be clearly explained to the unaccompanied child.

The proposed recast Eurodac Regulation contains amendments strengthening the duty to provide information. The requirement to provide information in writing, and where necessary, orally, in a language the data subject understands or is reasonably supposed to understand is complemented in Article 30 of the proposal with a duty to provide such information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". The type of information to provide is extended to include the contact details of the data protection officer, the retention period, and the right to lodge a complaint.

Article 2 (2) of the proposal underlines that children must be informed "in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting and facial image procedure" to them. They "shall be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image are taken". These safeguards are very important but need also to be implemented in practice.

In practice, child specific info leaflets are rare and authorities face challenges in providing child-friendly information. Unaccompanied children seeking asylum interviewed by FRA in the past remarked that they could not understand the information provided to them, indicating in some cases that even their own legal representatives did not always explain the procedures to them adequately.[37] Although not specific to Eurodac, a FRA research carried out with applicants for international protection noted that information is most effective when it is provided both in writing as well as orally.[38] Given that unaccompanied children will need to be accompanied by their guardian, it would be easy to ensure that oral information is given to them through the help of the guardian.

FRA Opinion 3

The proposed recast of the Eurodac Regulation contains important safeguards regarding information to be given to children. These could, however, be further enhanced by spelling

---

[35] *Ibid*., Article 12 (1).

[36] See: http://fra.europa.eu/en/project/2014/biometric-data-large-eu-it-systems-areas-borders-visa-and-asylum-fundamental-rights.

[37] FRA (2011), *Separated, asylum-seeking children in European Union Member States*, Luxembourg, Publications Office of the European Union, p. 63.

[38] FRA (2010), *The duty to inform applicants about asylum procedures: The asylum-seeker perspective*, Luxembourg, Publications Office of the European Union, pp. 19-20.

out a duty in Article 2 (2) of the proposed recast Eurodac Regulation to provide age-appropriate information to unaccompanied children also orally.

To facilitate an effective implementation of the safeguards included in the proposed recast Eurodac Regulation, the European Commission and relevant EU agencies could consider documenting and disseminating promising practices, for example, on the role of the guardian in supporting the provision of information.

2.2. Fingerprinting children: adding a child protection objective to Eurodac

Leaving aside the challenges in collecting biometric data from children in a child-friendly, gender-sensitive and respectful manner which is discussed in Section 1 the first question to examine is whether lowering the age limit of biometric registration from the current 14 years to six years is justified to achieve the purposes set out in Article 1 of the proposed recast Eurodac Regulation. Article 1 contains three purposes, namely: applying the Dublin system, combatting irregular immigration and fighting serious crime.

The collection of biometric data from children interferes with their right to respect for private and family life and with the right to protection of personal data, which are respectively set out in Article 7 and 8 of the Charter. To be lawful, such processing must be necessary and proportionate. In addition, when deciding whether or not to collect biometric data from children, under Article 24 of the Charter a primary consideration must be given to the best interests of the child.

The lowering of age from 14 to six years creates also an additional challenge which may have implications on the rights of the child, namely the need to assess whether a child is younger than six years of age or not. FRA does not have data on age assessment of young children but it can be assumed that also for them there is no scientifically reliable method to be used when documentary evidence is lacking.

For the following reasons and given the evidence available it seems difficult to conclude that the processing of fingerprints for children as young as six years of age is necessary and proportionate, if such processing is limited to the purposes set out in Article 1 of the proposed recast Eurodac Regulation. First, processing fingerprints to combat irregular immigration is unlikely to result in significantly more removals or other important immigration law enforcement actions of children between the age of 6 and 14 years.

Second, the proportionality of processing fingerprints of young children to apply the Dublin system is questionable, particularly if the changes to Article 10 (5) of the proposed recast Dublin Regulation (which envisage the transfer of the unaccompanied child back to the Member State where the applicant *first* lodged his or her claim) are not accepted due to their tensions with Article 24 of the Charter.[39]

Third, there is insufficient evidence of the need to process biometric data of children below the age of criminal responsibility to prevent, detect and investigate serious crime. Given that

[39] European Commission, *Proposal for a Regulation of the European Parliament and of the Council 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 (recast)*, Brussels, 4 May 2016 COM(2016) 270 final. For the tension with Article 24 of the Charter see FRA (2016), *Opinion of the European Union Agency for Fundamental Rights concerning the proposal for a revised Dublin Regulation (COM(2016)270 final; 2016/0133 COD)*, pp. 49-50

in a large majority of EU Member States (24 out of 28) the minimum age of criminal responsibility (also for serious crimes) is 14 years or above,[40] an EU-wide processing of biometric data of younger children to investigate serious crimes would not seem proportionate. When addressing the issue of blanket retention of biometric data by law enforcement authorities of persons not convicted of a crime in the case of *S. and Marper*, the ECtHR emphasised that this may be especially harmful in the case of children, given their special situation and the importance of their development and integration in society.[41] These arguments are also applicable – and possibly even more so – where law enforcement authorities access data that have been originally collected for other purposes, and in light of the additional vulnerability of asylum seeking children (see also Section 4.4 in relation to law enforcement access to Eurodac data in general). Although there may be some benefits to allow law enforcement to access children's data, the explanatory memorandum accompanying the proposed recast Eurodac Regulation does not sufficiently demonstrate a need to process biometric data of children below the age of 14 years for law enforcement purposes apart from child trafficking.

At the same time, storing younger children's biometric data in Eurodac would bring child protection advantages, particularly if accompanied by other measures. It could help detect and protect child victims of trafficking as well as trace and protect unaccompanied children who go missing, abscond or otherwise disappear.[42] The explanatory memorandum introducing the proposed recast Eurodac Regulation notes the benefit of processing young children's biometric data to trace missing children as well as families when those with young children get split in the EU – a phenomenon FRA regularly raises in its overviews of migration-related fundamental rights concerns in Member States that have been particularly affected by large migration movements.[43] It also notes potential value for the identification of child victims of trafficking.[44] In April 2016, the European Parliament discussed the growing concern of third-country national children going missing with FRA suggesting possible concrete actions, including a better use of SIS II.[45] More generally, being able to reconstruct

---

[40] The exceptions are France (13 years for serious crime), Ireland, the Netherlands and the United Kingdom. See European Commission (2014), *Summary of contextual overviews on children's involvement in criminal judicial proceedings in the 28 Member States of the European Union*, Table 3.1, p. 7.

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

[42] For a more detailed analysis on this issue, 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.

[43] See, for example, FRA September 2016 Monthly report, http://fra.europa.eu/en/theme/asylum-migration-borders/overviews/september-2016 – in Austria, Ministry of Interior officials consider the lack of fingerprinting of children below the age of 14 years to be an obstacle to identifying and tracing children in case they go missing – and FRA October 2016 Monthly report, http://fra.europa.eu/sites/default/files/fra_uploads/fra-october-2016-monthly-migration-focus-key-issues-0_en.pdf which describes the challenges in identifying and protecting separated children in many Member States, for example in Bulgaria and Greece.

[44] European Commission, *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)*, Brussels, 4 May 2016, COM(2016) 272 final, Explanatory Memorandum, (hereinafter European Commission, Explanatory Memorandum), pp. 4, 9 and 10.

[45] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Committee meeting debate, *The Fate of 10,000 missing refugee children*, 21 April 2016, available at: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160421-1500-COMMITTEE-LIBE and FRA (2016), Background note on

the life of an unaccompanied child since his or her arrival to the EU will also help in assessing the child's best interests. In a recent discussion paper, the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF) and the International Rescue Committee also noted that registration of unaccompanied children could include biometric data.[46]

The current experience with Eurodac shows, however, that taken alone the processing of children's fingerprints does not contribute significantly to their protection. 88% of all asylum applicants considered to be unaccompanied children in the EU-28 from 2008 to 2015 were aged from 14 to 17.[47] Most missing unaccompanied children are already in Eurodac. Nevertheless, they continue to disappear and are rarely traced. This is unlikely to change with the proposed recast Eurodac Regulation, as the only new purpose added to the IT-system is assisting with the control of irregular migration to or inside the EU. To be used as a child protection tool, Eurodac would need to pursue also a child protection objective – protecting child victims of trafficking as well as tracing and protecting missing children. In this manner, it could also contribute to the objective of the Victims Directive (2012/29/EU)[48] to safeguard the rights of child victims.

The tracing of missing children presupposes keeping track that a child has disappeared. This would require that all cases of missing children are reported to the police and entered in SIS II based on Article 32 of the Council Decision 2007/533/JHA on the establishment, operation and use of the second generation SIS.[49] In practice, this is not regularly done, due to unclear reporting responsibilities at national level, weak guardianship systems and other reasons. Since it will be impossible to store fingerprints in SIS II once the child has already disappeared, a prior processing of fingerprints in Eurodac would enable the authorities to have the fingerprints of all children from third countries, of whom the authorities are aware that they went missing.

Availability of information to ensure the protection of a child would need to be reconciled with strict rules limiting access to Eurodac. Current efforts to increase interoperability between IT-systems could be used to examine if it is technically feasible to enable accessing the data on missing children stored in Eurodac only by consulting SIS II. In this way, police or other authorities responsible to identify missing children would not need access to Eurodac but only to SIS II. Access to Eurodac could be limited to authorities responsible for the prevention, detection and investigation of trafficking in children as well as Europol. To further control access to biometric data of young children, the feasibility of using cryptographically transformed biometric identifiers could be examined.[50] This would mean that in a first step comparisons are made with the transformed biometric identifiers on a "hit"/ "no-hit" basis.

---

ways to prevent unaccompanied migrant children from going missing, available at: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-libe_missing_children_21_april_2016_background_note.pdf.

46 UNHCR, UNICEF, International Rescue Committee, *Discussion Paper on a Possible Way Forward to Strengthened Policies and Practices for Unaccompanied and Separated Children*, December 2016, p. 5.

47 Calculations based on Eurostat, table migr_asyunaa, extracted on 6.12.2016.

48 Directive 2012/29/EU of the European Parliament and of the Council of 5 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315, 14.11.2012.

49 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, 7.8.2007, pp. 63-84.

50 This concept is known as Biometric Template Protection. See also ISO Standard ISO/IEC 24745:2011 concerning biometric information protection.

The transformed biometric identifiers would in themselves not enable identification. Only in case of a match, the "raw" biometric information would be used, which would allow for the identification and exchange of further information on the person.

Moving to family tracing, the presence of family links is not envisaged among the additional data to be stored in Eurodac. Family links are only recorded in national IT-systems and, in future, in the centralised registration and monitoring system ("automated system"), to be set up under the proposed recast Dublin Regulation (but only for applicants for international protection).[51] The benefits of Eurodac would increase if family links data were treated in the same manner as the alphanumeric data which the recast proposal suggests to add to the system.

Tracing of missing children and subsequent family tracing[52] requires more than just storing biometric data and family links. Clear follow up duties are a precondition for realising the potential child protection benefits of Eurodac. When a child is found, follow up measures should include referral to child protection authorities, a needs assessment and the determination of a durable solution, together with any investigation which may be necessary if the child is a victim of serious crime. Efforts to trace unaccompanied children who went missing remains however only one of several actions which are needed to address this phenomenon, which must be accompanied by improving reception conditions, strengthening guardianship systems and gaining a better understanding of why children go missing and what can be done to prevent their disappearance. This will help avoid creating a vicious cycle where children are found and go missing again. It will also effectively protect them from violence, abuse and exploitation.

FRA Opinion 4

The proposed recast Eurodac Regulation suggests processing of children's biometric data as young as six years of age to achieve the purposes set out in its Article 1, namely: applying the Dublin system, combating irregular immigration and fighting serious crime. To comply with Article 7 (respect for private and family life), Article 8 (protection of personal data) and Article 24 (the rights of the child) of the Charter, this measure can only be justified if it expressly pursues a child protection objective. More specifically, it should serve to protect child victims of trafficking and support the identification and protection of unaccompanied children who go missing, disappear or abscond, as the European Commission highlighted in its explanatory memorandum accompanying the proposed recast Eurodac Regulation. Therefore, the following changes to EU law should be made:

- ***An additional purpose to protect child victims of trafficking in human beings and to identify and protect missing children should be added to Article 1 (as Article 1 (1) (d)). Only national law enforcement authorities responsible for the prevention, detection and investigation of child trafficking as well as Europol should be able to access Eurodac to protect child victims of trafficking in human beings. The question whether general law enforcement access under Article 1 (1) (c) to Eurodac for children under the age of 14 years is proportionate, should be assessed based on additional evidence of the relevance of these data for combating terrorism and other serious crime.***

---

[51] European Commission, *Proposal for a Regulation of the European Parliament and of the Council 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 (recast)*, Brussels, 4 May 2016 COM(2016) 270 final, Articles 22 and 44.

[52] In this context, see also the EASO practical guide on family tracing, March 2016.

- ***Personal data stored on children under the age of 14 years should be blocked for the purposes set out in Article 1 (1) (b).***
- ***Should additional alphanumeric data of applicants for international protection be included in the future version of Eurodac, consideration should be given to record also family links (including between separated children and an accompanying adult), so as to increase the system's potential to trace and reunite missed family members and justify the use of personal data stored on children under the age of 14 years for the purpose set out in Article 1 (1) (a).***
- ***An explicit duty should be included in EU law obliging Member States to record all children (under the age of 18 years) who have disappeared from reception facilities as missing persons in the Schengen Information System II (SIS II). As soon as a child is entered in SIS II as missing, his or her fingerprints and other personal data stored in Eurodac relevant for tracing missing children should, if feasible, become visible by consulting SIS II, without the need for authorities responsible for tracing missing children to access Eurodac.***
- ***A rule should be included in EU law, based, for example, on Article 81 (3) of the Treaty on the Functioning of the EU (TFEU), to oblige Member State authorities which identify a missing child to contact competent national child protection authorities to undertake a needs assessment with a view to find a durable solution for the child in line with his or her best interests.***

2.3. Reducing the risk of a false fingerprint match for young children

A sufficiently high quality of the captured fingerprints is a precondition for a reliable match. The processing of fingerprints of young children has been subject of recent research. The EU Joint Research Centre published a detailed report on the subject in 2013.[53] The report suggests that captured fingerprints of children who are at least six years meet acceptable quality standards. The study also demonstrated that reliable matches can be made up to five years after the fingerprints have been taken, but it did not draw conclusions of the reliability of a match when more than 5 years have passed.[54]

The degree of active co-operation of the person being fingerprinted directly impacts on the quality of the captured fingerprint and therefore on the match. This also means that the quality of information on the purpose of the fingerprinting provided to both the parents and the child will directly influence the reliability of the fingerprint match. This poses particular requirements on staff training.

The margin of error when comparing children's fingerprints must not be higher than for adults. In light of the current state of technology and the increasing risk of false matches, the ten years retention period seems excessive. False matches do not only undermine the functioning of the system as such but may also have disproportionate effects for children.

Fingerprints can be recorded in databases either as plain or rolled. For rolled fingerprints, the fingerprint images are obtained by rolling a finger from one side to the other ("nail-to-nail")

---

[53] Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen, *Study on Fingerprint Recognition for Children*, September 2013, available at: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20(pdf).pdf.

[54] *Ibid* p. 79.

to capture all of the ridge details of a finger. Plain or flat impressions are those in which the finger is pressed down on a flat surface but not rolled. Plain impressions cover a smaller area than rolled prints; they typically do not have the distortion introduced during rolling.[55] The Eurodac Regulation is ambiguous on what type of fingerprints to enrol. The Explanatory Memorandum says that Member States will continue to take the fingerprints of all 10 fingers as plain and rolled impressions (p. 13), whereas fingerprint data is defined in Article 3 (1) (n) as plain fingerprints or latent fingerprints.

Rolled fingerprints are of higher quality and can be used for criminal law enforcement purposes, for example, by comparing them with latent fingerprints found on the scene of crime. As shown in Table 1, VIS and the planned Entry-Exit System enrol plain fingerprints only.

Table 1: Intrusiveness of fingerprints processed in existing and future large-scale IT-systems

IT-system	No. of fingers	Type of fingerprint images	Source
Eurodac	10	plain + rolled	Explanatory memorandum, p. 13; Article 3 (1) (n) recast 2016 Eurodac Proposal
VIS	10	Plain	Articles 5 (1) (c), 9 (6) VIS Regulation, Annex Commission Decision 2009/756/EC
Planned entry-exit system (EES)	4	Plain	Recital 11, Article 3 (1), (15) EES Proposal, COM(2016) 194 [56]

Source: FRA (2016), based on EU (proposed) legislation

FRA Opinion 5

To respect the duty to give a primary consideration to the best interests of the child, fingerprints should not be compared anymore with those taken in the past if the likelihood of a wrong match increases. In case of young children, the reliability of matches of fingerprints after more than five years have passed is not yet proven.

To avoid the negative consequences of a possible mismatch after a certain period has elapsed, fingerprints of children younger than 14 years should only be automatically compared for a maximum of five years. Following this period, dactyloscopic experts should only carry out manually such comparisons to avoid disadvantages for the child.

Rolled fingerprints are of higher quality compared to plain fingerprints. Given the criminal law connotation of rolled fingerprints, however, the legislator should define the type of fingerprints to enrol in Eurodac.

---

[55] Jain, A. K., Feng, J. (2011). *Latent Fingerprint Matching*, IEEE Transactions on Pattern analysis and machine intelligence, Vol. 33, No. 1, January 2011, available at: https://www.researchgate.net/publication/47815470_Latent_Fingerprint_Matching.

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

2.4. Evaluating the effects of introducing facial image comparisons

Next to the lowering of the age as of which fingerprints are collected, the second main change relating to biometrics concerns the processing of facial images as a biometric identifier. Facial images are a common biometric identifier which is used, for example in ABC gates (automatic border control gates) and self-service kiosks by comparing the picture of the person to the biometric picture stored in national passports, so called eMRTDs or e-passports.[57]

At present, large-scale IT-systems established at the EU level do not process facial images as a biometric identifier, the planned Entry-Exit-System will do so.[58]

According to recital (10) of the proposed recast Eurodac Regulation, the rationale for processing two biometric identifiers in Eurodac lies in the need to mitigate challenges resulting from non-compliance with the obligation to give fingerprints.[59]

The proposed recast Eurodac Regulation takes a cautious approach giving priority to the matching of fingerprints and using the comparison of facial images as a last resort where the matching of fingerprints is not possible (recital (10), Article 16). Facial recognition will only be introduced following a technical feasibility study by eu-LISA to be carried out by 2020 (Article 42 (4)).

Facial recognition techniques have improved during the last years, but cases of lookalikes and twins may still lead to wrong matches. Also the length of time which passed between taking the picture and comparing it impacts on a correct matching. Changes in the facial shape of a child also impacts on the reliability of a match, for example, when the image of a six year old child is compared 5 years later on in time.[60]

To minimise any risks for false matches, all hits received when carrying out comparisons should always be checked and verified (both hits concerning fingerprints as well as facial images). To ensure reliability of matching results in particular for children, verification of hits concerning the facial image should be carried out not only when facial image is the sole biometric identifier (Article 16), but also when comparisons are made simultaneously with both fingerprints as well as facial images (Article 15).

The processing of facial images is primarily a tool to deal with persons who object to give their fingerprints. It is difficult to assess whether this category of people will resort to other forms of self-harm to avoid that their facial image will be taken and whether parents would inflict harm on their children to avoid that facial images will be successfully taken.

---

[57] eu-Lisa, (2015), *Smart Border Pilot Final Report: Report on the technical conclusions of the Pilot*, Volume 1, Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_report_on_the_technical_conclusions_en.pdf.

[58] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No. 767/2008 and Regulation (EU) No 1077/2011, Brussels, 6 April 2016, COM(2016) 194 final, Art. 14(1)(f), 21(2).

[59] See also European Commission, Explanatory Memorandum, p. 13.

[60] Aashmi, Sakshi Sahni, Sakshi Saxena (2014): Survey: Techniques for Aging Problems in face recognition, *MIT International Journal of Computer Science and Information Technology,* Vol. 4, No. 2, August 2014, pp. 82-88, available at: http://www.mitpublications.org/yellow_images/1411547948_logo_Paper-8.pdf; Narayanan Ramanathan, Rama Chellappa, Soma Biswas (2009): Computational methods for modelling facial aging: A survey, *Journal of Visual Languages and Computing 20*, pp. 131-144.

FRA Opinion 6

The comparison of facial images in Eurodac should only be used as an additional feature when determining the identity of a person. This is particularly important for children. A comprehensive assessment of how the processing of facial images affects a person's fundamental rights should include a review of the reliability over time of facial images of younger children. It should also consider possibly harmful practices persons may resort to in order to avoid that their facial image or the image of their children be successfully taken.

Following a hit after having simultaneously compared fingerprints and facial image, in accordance with Article 15, both biometric identifiers should always be subject to checks and verifications. The EU legislator should consider making this explicit in Article 26 (4) and Recital 31, which would minimise any risks for false matches.

The EU legislator should consider amending Article 42 (4) of the proposed recast Eurodac Regulation and make recommendations for the introduction of facial recognition technology subject to a comprehensive evaluation of the impact the processing of facial images has on fundamental rights. FRA would be ready to support such an evaluation.

2.5. Making the impact of Eurodac on children understandable

Under Article 9 of the proposed recast Eurodac Regulation, eu-LISA will be required to provide monthly Eurodac statistics on data transfers, various types of hits, the number of fingerprints which had to be requested again (due to poor quality), data sets marked, unmarked, blocked and unblocked. No sex or age breakdown is requested for these statistics.

Some of these statistics will help to capture secondary movements – e.g. those in Article 9 (1) (b), (c) and (d)). Other statistics – such as those in Article 9 (1) (e) (j) and (k) – will reveal quality issues relating to the biometric identifier. Statistics under Article 9 (1) (h) and (i) concern requests for access by law enforcement authorities and Europol.

Lack of breakdown of statistics by age and gender will make it difficult to assess how the implementation of Eurodac affects children. An age breakdown of statistics concerning the matching difficulties (Article 9 (1) (e) and (k)) would make it possible to assess the reliability of biometric matching for boys and girls. Similarly, Articles 5 and Article 20 (3)-(5) of the proposed recast Dublin Regulation envisage various restrictive measures for persons who moved on to another Member State without authorisation. Taking into account the impact of these measures on children[61] it would be helpful to publish regular data on the number of children affected by it. The same applies to cases in which law enforcement authorities request access to children's data stored in Eurodac.

FRA Opinion 7

To evaluate better the impact of the Eurodac Regulation on children, monthly statistics provided by eu-LISA under Article 9 of the proposal should be broken down by age and sex to understand how many boys and girls under the age of 18 years are affected. Children's statistics concerning the reliability of biometric matching should be broken down by year of birth.

[61] FRA, *Opinion of the European Union Agency for Fundamental Rights on the impact on children of the proposal for a revised Dublin Regulation (COM(2016)270 final; 2016/0133 COD)*, 23 November 2016.

3. The right to asylum

Article 18 of the Charter guarantees the right to asylum. This section analyses selected provisions of the proposed recast Eurodac Regulation which are related to the right to asylum. It first examines possible safety risks of an enhanced Eurodac for asylum seekers (but also for their families in the home country), looking first at the provisions for sharing data with third countries and subsequently at the plan to store significantly more alphanumeric data in Eurodac. The considerations covered in this section affect also children.

3.1. Managing data transfers to third countries without exposing people in need of international protection to risks

Personal information which can allow the country of origin to deduce directly or indirectly that a person has applied for asylum in another country is extremely sensitive as it can expose the person concerned and/or his or her family members – including children – remaining in the country of origin to retaliation measures. This was also confirmed by UNHCR, which stated that confidentiality of data is particularly important for refugees and other people in need of international protection, as there is a danger that agents of persecution or rights violations may ultimately gain access to such information, potentially exposing a refugee to danger even in his/her asylum country.[62] In some case, the sharing of such information may also create a *sur place* refugee claim.[63]

At the same time, if Member States are to return rejected international protection applicants or to request their re-admission following a negative admissibility decision (for example, based on the concept of safe third country), they must be allowed to use personal information available to them to identify the individual or obtain travel documents from the country of origin. Personal data needed for this purpose (name, date and place of birth, travel document details) – which is currently stored in national databases – would in future also be directly available in Eurodac.

Following a match, Article 38 of the proposed recast Eurodac Regulation will allow Member States to share with third countries personal data stored in Eurodac on a specific individual. All data "necessary in order to proof the identity of third-country nationals for the purpose of return" may be shared, except for the information that the individual applied for asylum (proposed Article 38 (3)). This means that data which are not needed for this purpose, such as the unique identification number (meaning the number which allows to link the Eurodac file to the personal data stored on the individual in national databases), for example, may not be shared.

As not only the fingerprints, but also alphanumeric data will in future be available to law enforcement authorities, the likelihood that personal data are further shared with third countries

---

62 UN High Commissioner for Refugees (UNHCR), *UNHCR comments on the European Commission's Proposal for a recast of the Regulation of the European Parliament and of the Council 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 ("Dublin II") (COM(2008) 820, 3 December 2008) and the European Commission's Proposal for a recast of the Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [the Dublin II Regulation] (COM(2008) 825, 3 December 2008)*, 18 March 2009, available at: http://www.refworld.org/docid/49c0ca922.html [accessed 5 December 2016].

63 This concerns persons who leave their own country for non-refugee related reasons but acquire a well-founded fear of persecution once they are already in the host country. See UNHCR, Refugee Protection and International Migration, http://www.unhcr.org/4a24ef0ca2.pdf, paras. 20-21.

after becoming part of law enforcement files increases, for example, in the framework of bilateral cooperation.

Unambiguous rules are needed to enable Member State to share personal data stored in Eurodac with third countries without putting individuals or their families at risks of serious harm by actors in the country of origin.

Sharing personal data of an applicant for international protection with the country of origin to initiate a return procedure before the asylum claim has been rejected in the final instance may put the applicant's safety in jeopardy and should therefore be avoided.

Article 37 (2) of the proposed recast Eurodac Regulation, bans the transfer of personal data to third countries if there is a real risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights. This is an important safeguard, which in the current wording concerns only personal data which are exchanged between Member States following a match in Eurodac.

Article 38 (1) of the proposed recast Eurodac Regulation allows the transfer only if a third country gives assurances concerning the use of the data and provided the data subject has been informed that his or her personal data may be shared with a third country. The third country must explicitly agree "to use the data only for the purpose for which they were provided and to what is lawful and necessary [for the readmission] and to delete that data where it is no longer justified to keep it". The practical implementation of such legal safeguards may be challenging. Article 37 (3) of the new Data Protection Directive[64] contains a provision which requires transfers of data, (including also the justification for the transfer) to be documented and made available to the supervisory authority upon request. A similar rule should be considered for Eurodac.

FRA Opinion 8

When personal data processed in Eurodac are shared with third countries, sufficient safeguards must be in place. Such safeguards are required to avoid exposing applicants for international protection and their families to risks of serious harm by actors in the country of origin, as well as to comply with the right to protection of personal data enshrined in Article 8 of the Charter. For this purpose, the following measures should be considered:

- ***Article 38 (1) of the proposed recast Eurodac Regulation should be amended to exclude sharing personal data of asylum applicants with their country of origin to prepare their return as long as no final decision has been taken on the application for international protection;***
- ***Article 37 (2) contains an important fundamental rights safeguard that should also apply to personal data stored in Eurodac and not only to data exchanged between Member States.***

Personal data that can be transferred to third countries should be expressly listed in Article 38. Data that are not needed for the purpose of return, such as the unique identification number or data on Dublin transfers should be excluded from the list of transferable data.

---

[64] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89-131.

When the transfer of personal data to third countries concerns applicants for international protection, the EU legislator could require Member States to document the transfer and its justification, and make such documentation available to the data protection supervisory authority on request, similarly to what is envisaged in Article 37 (3) of the new Data Protection Directive.

3.2. Reducing the risk of information leaks

The proposed changes to the recast Eurodac Regulation (Articles 12 – 14) expand significantly the personal data to be processed. Currently, the Eurodac database only contains fingerprints, sex and the personal reference number of the data subject (in addition to some circumstantial information). In future, pursuant to proposed Articles 12, 13 (2) and 14 (2) the name, surname, nationality, date and place of birth, as well as information on the travel document, will also be processed in Eurodac. Today, this information is stored in national databases and can only be linked to the fingerprints in Eurodac through the personal reference number. The proposed change would transform Eurodac from a database of fingerprints into a database containing basic personal data and travel document details of all asylum applicants and migrants in an irregular situation apprehended in the EU and the Schengen area.

Taken together with the proposed changes to the Dublin Regulation (which propose to establish a centralised registration and monitoring system, where all asylum applications lodged in the Dublin area are registered under a unique identification number),[65] the new framework will provide a comprehensive picture of who applied for asylum and where during the last 10 years.

The existence of a central place where personal data of all asylum seekers are stored can be extremely attractive to countries of origin who may be looking, for example, for the whereabouts of their political dissidents. The increase of personal data envisaged for storage under the proposed Eurodac recast Regulation intensifies the risks for the data subject in case of unlawful use.

Unlawful sharing of information stored in databases can expose the data subject to other risks, as illustrated by interviews carried out by FRA for its project on biometrics.[66] The easy access to personal data stored in databases concerning asylum applicants was highlighted by, for instance, experts providing legal advice in Germany: "*I only have to know the name and the date of birth of a given person, maybe the case number, and can get data which has been recorded in such systems from the police or other authorities, without power of attorney. I do it all the time. I do have power of attorney for that, but nobody asks for it.*" The same expert mentioned that in cases of domestic violence, there is a risk that easy access means that the perpetrator extracts information from authorities which the person in fact should not have been given. There is a need for robust data security measures and strict supervision of their implementation to prevent unlawful access and data leakages.

The Eurodac Regulation contains safeguards to reduce the risk of unlawful processing of the personal data stored. For example, according to proposed Article 28 (1), a Member State will not be able to access personal data recorded by another Member State, except for the data

---

[65] European Commission, *Proposal for a Regulation of the European Parliament and of the Council 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 (recast)*, Explanatory Memorandum, Brussels, 4 May 2016 COM(2016) 270 final, Articles 22 and 44.

[66] For a brief description of the project see FRA's webpage at http://fra.europa.eu/en/project/2014/biometric-data-large-eu-it-systems-areas-borders-visa-and-asylum-fundamental-rights.

it receives when sending a person's fingerprint (and in future, a facial image) for comparison. Under the current system, when there is a match, the requesting Member State receives only a confirmation that the person has already been processed in Eurodac and a reference number through which it can contact the Member State of origin to receive further personal data. The rationale of not making this information automatically available to the Member State concerned is to introduce a further step before having access to the asylum applicant's name, nationality, date and place of birth and other personal data to ensure that it is only accessed when really needed.

This additional step could be seen as unnecessarily cumbersome for return purposes. As soon as an application for international protection is rejected, the personal data becomes less sensitive. For migrants in an irregular situation the risk of possible negative consequences is reduced and it would therefore seem proportionate to allow the requesting Member State to see directly the full set of personal data, including travel document details, stored. A distinction should therefore be made between personal data on asylum applicants and personal data concerning other categories of persons maintaining the current two-step approach for asylum applicants.

FRA could not find any source which indicates that the purpose of determining the Member State responsible to examine an asylum application could not be achieved with the current decentralised approach where most personal data are stored only at national level and not in Eurodac. The two-step approach would therefore not undermine the effective implementation of the Dublin system.

FRA Opinion 9

Eurodac needs to be immunised against unlawful access to personal data of applicants for international protection. Abusive access to personal data stored in Eurodac by the country of origin would undermine the right to asylum enshrined in Article 18 of the Charter. It may also expose family members, including children, who remained in the country of origin to acts of retaliation to force dissidents to come back home or enable the kidnapping of applicants for international protection.

The EU legislator should carefully assess the necessity and proportionality of centrally storing the name, surname, nationality, date and place of birth, as well as information on the travel document of an applicant for international protection for a period as long as 10 years. To reduce risk of abuse, the EU legislator should consider blocking the personal data of international protection applicants listed in Article 13 (2) (c)-(e) and (h) of the proposal until the international protection claim is rejected in the final instance that these are not automatically visible in case of a Eurodac match. Where such data are needed to achieve the objectives laid down in Article 1 (1) (a) and (c) of the proposed recast Eurodac Regulation, it should be exchanged bilaterally between Member States as it is currently the case under Regulation (EU) No. 603/2013.

3.3. Clarifying Articles 15 (4) and 16 (5)

Article 15 (4) of the proposed recast Eurodac Regulation lays down a new rule stipulating that where a fingerprint match indicates that an asylum application has been made in the European Union, "that evidence shall take precedence over any other hit received." The same rule is echoed in Article 16 (5) of the proposal in relation to facial image hits.

The formulation of this rule creating a sort of hierarchy between hits is quite vague and ambiguous, therefore allowing for multiple interpretations. Departing from the ordinary meaning of the terms in the draft provision, this wording could be understood that Eurodac

hits would trump hits on valid or expired visas found in the Visa Information System (VIS). It thus would go against the hierarchy of criteria established by the Dublin Regulation in force ((EU) No. 604/2013) and maintained by the proposed recast Dublin Regulation (COM (2016) 270 final).

The explanatory memorandum to the proposal gives guidance on the interpretation of the proposed rule in Article 15 (4) and 16 (5). It is to ensure that where multiple hits are retrieved from the Central System of Eurodac relating to the same individual, the Dublin procedure is followed by the Member State that conducted the search, and not a return procedure is initiated against that individual. Put differently, it guarantees that the Member State having consulted Eurodac is left in no doubt about the correct procedure to carry out. It flows from the above regulatory logic that this provision aims at remaining within the ambit of the Eurodac system and covering only hits retrieved from within Central System of Eurodac. In other words, Articles 15 (4) and 16 (5) are not designed to affect the core question of determining the responsible Member State and do not give priority to certain criteria/evidence during the Dublin phase; they apply one step prior, before triggering the Dublin mechanism. Consequently, a Eurodac hit is not meant to override all other hits found in different databases, such as VIS. However, these provisions need to be rephrased so as to reflect better and in clearer terms their real purpose.

FRA Opinion 10

The provisions in Articles 15 (4) and 16 (5) of the proposed recast Eurodac Regulation which deal with the way to handle cases of multiple matches could be interpreted in different ways.

For the sake of normative clarity and enhanced coherence between connected legislative instruments, these provisions should be rephrased, in line with the explanatory memorandum to the proposed recast Eurodac Regulation. The EU legislator should make it explicit that the new rule ('hierarchy of Eurodac hits') reflects without prejudice to the hierarchy of criteria as laid down in the Dublin Regulation.

4. Respect for private life, data protection and access to justice

The right to respect for private life (Article 7), the right to the protection of personal data (Article 8) and the right to an effective legal remedy, notably judicial review (Article 47) are protected by the Charter regardless of nationality and the third-county nationals' migration status. These Charter rights are thus applicable to everyone, including those third-country nationals whose fingerprints have been introduced into Eurodac. Recording and storing data in large-scale IT-systems in the field of migration and asylum raises always serious legal questions on how to reconcile the immigration law enforcement and security related purposes of such databases with the data subjects' rights to the respect for private life, data protection and access to justice. Although the right to private life and the protection of personal data might be limited pursuant to the Charter, for interferences with such rights to be justified, they have to respect the requirements of Article 52 (1) of the Charter. These are the following: the limitations must be provided for by law; must genuinely meet objectives to general interest recognised by the EU or the need to protect the rights and freedoms of others; respect the essence of the rights and be proportionate.[67] This section deals first with the risk of duplicating the processing of personal data unnecessarily, the double storing of fingerprints and subsequently with how to address the issue of incorrect data stored. In addition, it looks at the proposed changes to Eurodac in light of law enforcement access to the system and the existing safeguards.

4.1. Avoiding multiple processing for the same purpose

The proposed recast Regulation expands the scope of Eurodac by including a new purpose in Article 1 (1) (b), namely to "assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation." This transforms Eurodac from a database to assist in applying the Dublin system into a migration management database, merging protection objectives with immigration law enforcement.

Having a tool which serves both objectives is not new. Many foreigners' databases at national level have been set up to manage asylum procedures and to serve immigration law enforcement. In these cases asylum authorities and aliens police have access to different parts of the data, ensuring that sensitive asylum-related information is not accessible to non-asylum authorities.

At the EU level, there is no specific IT-system dedicated to combatting irregular migration, only. However, information relevant for immigration law enforcement is scattered in different databases. As illustrated in Table 2, there are four large-scale IT-systems which (once established) will have immigration law enforcement among their purposes. The SIS II system contains entry bans and will soon be used to store return decisions as well.[68] The Entry-Exit System will flag persons who exceeded the allowed period for short-term stay (maximum 90 days within 180 days). Authorities who apprehend a migrant in an irregular situation can check his or her personal details against VIS.

---

[67] See also e.g. CJEU, C-429/14, *WebMindLicenses Kft. v. Nemzeti Adó-és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 December 2015, paras. 69, 80-82.

[68] European Commission, *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*, Brussels, 21.12.2016, COM(2016) 881 final (2016/0407 (COD)). See also European Commission, *Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security*, COM (2016) 205 final, 6 May 2016, p. 7.

Table 2 lists the relevant provisions in these four IT-systems.

Table 2: Immigration law enforcement purposes as reflected in existing and planned EU IT-systems

Purpose	Provisions in the relevant information systems regulating the different purposes			
	Eurodac	SIS II	EES	VIS
Apprehension and return; checks and identification of migrants in an irregular situation	Articles 1 (1) (b) and 14	Articles 1 (2), 27 (b) and proposed Articles 1, 3-7 in COM(2016) 881 final	Articles 1 (1), 5 (b), 5 (c), 24, 25	Articles 2 (e), 19 and 20

Source: FRA (2016), based on EU legislation

Article 5 of the General Data Protection Regulation (Regulation (EU) 2016/679)[69] spells out the principle of data minimisation whereby personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". It would be difficult to conclude that storing the same personal data for the same purpose in different IT-systems is necessary. A careful assessment should be made to understand what added value using Eurodac for immigration law enforcement – in particular removals – would bring.

Recitals (12) and (13) of the proposal underline the value of personal information stored in Eurodac to identify and re-document migrants in an irregular situation so as to facilitate their return to the country of origin or their readmission to a third country. At a first sight, it seems that the value of Eurodac to facilitate returns is limited to those persons who entered the Member States' territory in an irregular manner – as personal data of those who entered lawfully can already be found in VIS or (with regard to visa-free nationals) will in future be available in the Entry-Exit System.

The immigration law enforcement purpose of the proposed recast Eurodac Regulation is formulated in a broad manner. The wording "assist with the control of illegal immigration" can have disproportionate effects on children who as a result of actions by their parents or care takers have crossed the border in an irregular manner. Storing personal data of persons who are apprehended within the territory in Eurodac is likely to contribute to driving migrants in an irregular situation further underground. FRA has in this context noted that migrants in an irregular situation avoid contacts with public services due to the fear of detection. The envisaged measure could further discourage them to contact medical facilities or lead them to refrain from sending their children to schools, thus resulting in disproportionate effects on children's fundamental rights.

Any period of irregular stay in the EU territory will negatively influence the trustworthiness of a request to enter or stay in the EU. According to Article 18 of the proposed ETIAS[70] – a system for visa-free third-country nationals to request prior authorisation to travel to the EU – a request for entry will automatically be compared with various EU databases, including Eurodac. For example,

---

[69] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1-88.

[70] European Commission, *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*, Brussels, 16 November 2016, COM(2016) 731 final.

a child planning to go on a school trip to the EU would risk not getting the travel authorisation through ETIAS, if a few years before she was processed in Eurodac when she was in the EU together with her parents, even if there is no entry ban against her.

Finally, the language that criminalises migrants in an irregular situation should be avoided, therefore the term irregular immigration is preferred over the term illegal immigration, as FRA noted in its project on the rights of migrants in an irregular situation.

FRA Opinion 11

The new purpose of Eurodac to "assist with the control of illegal immigration [...] and secondary movements" must be seen in light of other existing and planned information technology (IT)-systems that also pursue such objectives. Used together with other IT-systems, the broad definition of this purpose may result in a disproportionate negative impact on children.

It would therefore be advisable to formulate Article 1 (1) (b) of the proposed recast Eurodac Regulation in stricter terms by deleting the following part of the sentence "with the control of illegal immigration to and secondary movements within the Union and".

Moreover, it would be advisable to replace the term illegal immigration with "irregular immigration" throughout the proposed recast Eurodac Regulation.

4.2. Avoiding double fingerprinting

Articles 10 and 13 of the proposed recast Eurodac Regulation require Member States to process fingerprints of every applicant for international protection as well as of every third-country national who is apprehended in connection with his or her irregular border crossing. FRA observed that at the external borders newly arrived persons who expressed the intention to apply for asylum are often fingerprinted for Eurodac twice, first as irregular border crossers and subsequently as international protection applicants. This is particularly the case where the asylum application is formally lodged at a later stage, sometimes after transfer to another location. Double fingerprinting could amount to an unjustified interference into the right to respect for private life protected by Article 7 of the Charter and Article 8 of the ECHR. Repeating the fingerprinting exercise may sometimes be delicate. For example, earlier in 2016, FRA observed that people who after weeks of protest in Lampedusa agreed to give their fingerprints were transported to a relocation facility in Sicily, where as a first step they had to give their fingerprints for Eurodac again.

Present practice is to re-take rolled fingerprints of each of the 10 fingers, a process which requires the collaboration of the person concerned. Such double fingerprinting increases situations of possible tensions between individuals and the authorities and if avoided, reduces the risk of tensions relating to the fingerprinting process. The proposed fingerprinting of children as of six years of age may raise additional challenges, given the need to ensure that fingerprints are taken in a child-friendly manner.

One option to explore could be to redesign the system so as to enable Member States to register new arrivals who make an application for international protection but who have formally not lodged it yet as applicants for international protection under Chapter II of the Eurodac Regulation. This would require the system to accept an entry under Chapter II also when the information of the place and date of lodging the application for international protection are not yet available. Alternatively, consideration could be given to recording the place and date of expressing the intention to apply for international protection.

FRA Opinion 12

In many cases, asylum seekers who enter the EU in an irregular manner are first fingerprinted as irregular border crossers. When they formally lodge a claim for international protection, they are fingerprinted again as applicants for international protection. Double fingerprinting could lead to an excessive interference into the right to respect for private life enshrined in Article 7 of the Charter and Article 8 of the European Convention on Human Rights (ECHR). It could also create situations of tensions leading to the use of coercive measures to enforce fingerprinting.

To avoid having two separate entries of the same person, consideration could be given to allow the recording of persons apprehended in connection with their irregular crossing of the external border who express the wish to apply for asylum ("make" an application) as applicants for international protection, even when under national law the application is formally lodged only subsequently. This would also help to ensure that an asylum request is visible in the system from the beginning, which can increase protection from refoulement.

4.3. Reviewing correctness of data stored

Pursuant to Articles 12, 13 (2) and Article 14 (2) of the proposed recast Eurodac Regulation, a significant amount of alphanumeric personal data will be stored in the central system. In the absence of valid travel documents, such data will be collected during individual identification interviews and based on the information provided by the person concerned. Particularly in cases of large numbers of arrivals, FRA has observed that such initial police interviews may take place in stressful situations, and sometimes without adequate interpretation.[71] Mistakes are therefore not unlikely. For unaccompanied children, particularly if they are young, the risk of mistakes is even higher, as they may not know some of the information they are requested to provide.

According to Article 17 of the proposed recast Eurodac Regulation, personal data will be stored in the IT-system for ten years in case of applicants for international protection and for five years for other persons. Mistakes contained in the system may therefore have an impact for the individual also several years later where they can have unintended consequences, for example when they apply for the renewal of a residence permit or for a Schengen visa. In future, mistakes in the alphanumerical data included in Eurodac will have a greater impact as the data are not stored nationally but in a single centralised system, accessible by all EU Member States.

In its research on the risks and opportunities of using biometric data for migration management purposes, FRA noted the tendency to consider data stored in a system that also contains biometrics to be absolutely reliable. An expert providing legal advice to asylum seekers in Sweden, interviewed by FRA for its biometric project, pointed out that alphanumeric information linked to the fingerprint registration is treated as the 'truth' once it is registered in the system, regardless of the situation under which it was registered, or the mistakes that might have been committed when inserting it.

The same expert also reported mistakes concerning the date of birth of children on the basis of which the decision to register a child in Eurodac, or not, was taken and pointed to the difficulties in correcting a registration done by another Member State, as new information

---

[71] FRA (2014), *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, p. 88.

provided is often disregarded. A German NGO interviewed by FRA also noted that incorrect alphanumeric data may have critical consequences in the case of unaccompanied children (for which age is critical) and family reunification: *"Of course it is hard, if you are registered with a wrong name, because it has been recorded wrongly, to conduct a family reunification. When all documents, which one can provide, show different data…"*

It can be assumed that data subjects will rarely know that there are mistakes in the IT-system and hence not request their correction, making the right to an effective remedy under Article 47 of the Charter illusory. The issuance of a residence permit under Article 24 of the Qualification Directive[72] or Article 6 (4) of the Return Directive[73] would constitute a good opportunity to review the accuracy of data stored and initiate a correction *ex officio*.

FRA Opinion 13

Eurodac registrations may often be carried out under time pressure in situations of stress. Newly arrived asylum seekers and migrants may not yet trust the authorities and, therefore, may provide incorrect personal data. This is likely to lead to a significant amount of incorrect personal data being stored in Eurodac, particularly as alphanumeric data will also be stored.

To reduce the negative impact of mistakes contained in Eurodac, a duty to review the accuracy of data stored and to rectify possible mistakes could be inserted in Article 28 of the proposed recast Eurodac Regulation, for example, when issuing a residence permit or a return decision to the third-country national.

4.4. Ensuring proportionality of law enforcement access in light of the expanded scope of data

In its original form, the Eurodac Regulation was conceived to assist in the detection of multiple asylum applications and unauthorised entry. As such, access to data was restricted to immigration and asylum authorities. In 2013, the Eurodac Regulation was amended to introduce the possibility for Member States' law enforcement authorities and Europol to access Eurodac for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences. According to the explanatory memorandum of the proposal tabled by the European Commission in May 2012, law enforcement access for Eurodac was "needed as part of a balanced deal on the negotiations of the Common European Asylum System package."[74]

---

[72] Directive 2011/95/EU of the European Parliament and Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (recast), OJ L 337, 20.12.2011, pp. 9-26.

[73] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008, pp. 98-107.

[74] European Commission (2012), *Amended proposal for a Regulation of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)*, COM(2012) 254 final, 30 May 2012, p. 14.

The proposal to add a secondary objective not envisaged in the original architecture of the system raised considerable concerns. In its opinion, the European Data Protection Supervisor (EDPS) argued that the necessity and proportionality of law enforcement access were not sufficiently demonstrated and applicable data protection law aspects had not been sufficiently considered. In particular, it argued that the additional purpose of Eurodac presented a 'function creep'[75] and was hard to reconcile with the principle of purpose limitation,[76] and that the access to a database of vulnerable persons (international protection applicants) was potentially discriminatory.[77]

The concerns raised by the EDPS and other bodies led to the inclusion of additional safeguards. The national verifying authorities processing the requests for comparisons may in practice be part of the same organisational structure as the designated authorities submitting these requests, but need to act independently and be separate from the operating units (Article 6 (1) of Eurodac Regulation (EU) No. 603/2013). VIS has been added among databases that need to be consulted prior to the check of Eurodac and a more explicit delineation of conditions under which law enforcement agencies may request a comparison with Eurodac data has been included (Article 20 (1) of Eurodac Regulation (EU) No. 603/2013).

As a result, law enforcement access to Eurodac is currently accompanied by a broad set of safeguards. The access is indirect, based on submitting requests for comparison of data to a verifying authority and only receiving further information in case that there is a match with the fingerprints contained in Eurodac ('hit/no-hit system'). According to Article 20 (1) of Eurodac Regulation (EU) No. 603/2013, a request to Eurodac can only be made if the identity of the data subject has not been established by consulting other relevant databases (in case of the Member States, these are the national fingerprint databases, databases of other Member States available via the Prüm system,[78] and VIS). The request must be based on a legitimate purpose: it is only permitted where the comparison is necessary for the prevention, detection or investigation of terrorist offences or of other serious criminal offences, is necessary in a specific case and there are reasonable grounds to consider that the comparison will substantially contribute to this purpose, which exist particularly where there is "a substantiated suspicion" that the fingerprints of a suspect, perpetrator or victim of a terrorist offence or other serious criminal offence can be found in Eurodac. Similar principles apply to Member States' law enforcement authorities and to Europol.

The overall evaluation of Eurodac to be performed by the European Commission under Article 40 of Eurodac Regulation (EU) No. 603/2013 will also assess the impact on fundamental rights. Such assessment should also cover possible indirect discrimination in the framework of law enforcement access, and assess the continuing validity of the underlying rationale and any implications for future operations. Given that the first

---

75 European Data Protection Supervisor (2012), Opinion of the European Data Protection Supervisor on the amended 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 [.../...] [.....] (Recast version), 5 September 2012, paras. 26-27.

76 *Ibid.,* para. 28.

77 *Ibid.,* paras. 37-38.

78 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 was integrated in EU, and the implementing Council Decision 2008/616/JHA, transpose 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.

evaluation is only to be conducted in 2018, this important assessment has not yet been made and cannot inform the proposed changes.

The proposed recast Eurodac Regulation does not introduce major modifications to the existing model of law enforcement access beyond reflecting the planned extension of the system to also cover facial images. The overall increase in the scope of data to be covered in Eurodac, however, would result in significantly expanding the amount and type of information that would become available to law enforcement, covering also persons found irregularly staying in the EU territory and children as of the age of six, prolonging the storage periods and introducing new categories of data to be included directly in Eurodac.

The principle of proportionality under Article 52 (1) of the Charter applies to all rights guaranteed by the Charter, including the right to respect for private life and protection of personal data set forth in Articles 7 and 8 of the Charter and in Article 8 of the ECHR. The CJEU has provided interpretation of the principle of proportionality in relation to law enforcement access to data and the right to private life and protection of personal data in several rulings, most notably in the *Digital Rights Ireland* case[79] which led to the invalidation of the Data Retention Directive (Directive 2006/24/EC).

Already at present, Eurodac provides Member States' law enforcement agencies and Europol with access to a comprehensive set of data on third-country nationals that is not available for own nationals. 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. Therefore, a logical connection between the nature of the data and law enforcement exists.

Such logical link is not clearly given in case of law enforcement access to Eurodac. Although specific individuals whose data are included in the system may be connected to organised crime or even terrorism, these persons represent a small segment in the overall amount of data available in Eurodac. There is no prior evidence when including an individual in the database that the risk is higher than in the general population of the Member States. 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.[80] Furthermore, the ruling required that a differentiated retention (storage) period is established on the basis of the possible usefulness of the data for the purposes of the law enforcement objective.[81]

Although the data in Eurodac is primarily collected for a different purpose, the secondary law enforcement objective necessarily implies the need to take into account the principles outlined in the CJEU jurisprudence. This is particularly important given that a large share of persons included in the Eurodac database are applicants for international protection. The rate of successful applications for international protection among persons who have arrived to the EU in the last years[82] clearly indicates that the majority of persons included in Eurodac pursuant to Chapter II of the proposed recast Eurodac Regulation are persons in need of

---

79 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014. 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.

80 *Ibid.,* paras. 58 and 59.

81 *Ibid.,* para. 63.

82 In 2015, out of all 593,140 first instance decisions on asylum applications, 52 percent were positive decisions. With 39 percent, more than one in three decisions resulted in granting Geneva Convention refugee status. The rates of all decisions from 2008 to 2015 taken together are 37 percent positive decisions and 21 percent Geneva Convention refugee status. Source: FRA calculations based on Eurostat table migr_asydcfsta, extracted on 6.12.2016.

special protection. Given that their data are collected for a different purpose and without any connection to a criminal activity or another security risk, safeguards accompanying the access of law enforcement to this data should be particularly robust.

It is therefore essential that access of Member States' law enforcement agencies and Europol to the data remains subject to the existing safeguards contained in Eurodac Regulation (EU) No. 603/2013. A clearly defined purpose of combating terrorism and serious crime in a specific case (so that Eurodac cannot be used for profiling purposes) and a substantiated suspicion that the fingerprints or, in the future, facial image in the possession of the law enforcement authorities, belong to a person whose data are stored in Eurodac, are vital in light of the origin and nature of the data and the principle of purpose limitation. The indirect model of access by means of the hit/no-hit system becomes particularly relevant given the planned inclusion of additional alphanumeric data. An extension of scope of the available information accompanied by a reduction in safeguards would therefore be difficult to justify legally, particularly in the absence of the evaluation of the fundamental rights impact envisaged in Article 40 of Eurodac Regulation (EU) No. 603/2013. This issue needs to be taken into account also in the context of discussions on future interoperability of EU large-scale IT-systems including Eurodac, SIS II and VIS. In this framework, 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.

Retaining the harmonisation between the conditions for access by Member States' law enforcement authorities and Europol is another important element, which was already demonstrated in the discussions on the 2012 proposal of the European Commission which eventually led to aligning the access conditions.[83] So far, however, Europol has not found a technical solution to connecting to Eurodac in line with the existing conditions which include making requests for comparison through the National Access Point of a Member State rather than by means of an own channel of access to the Central System. This issue should be addressed, also to realise the child protection benefits of Eurodac.

In addition, as further information is to become accessible for law enforcement due to being included in Eurodac for migration-related purposes, the proposal should assess the consequences of granting such access and demonstrate the necessity and proportionality of such 'collateral' extension. In this regard, the proposal should examine in particular detail the impact of the CJEU jurisprudence requirement that a distinction is made between the different categories of data in terms of conditions of access and the length of retention based on their law enforcement relevance, taking into account that the longest retention period is foreseen for applicants for international protection, a category of persons who are in a vulnerable situation. Moreover, both under the current Eurodac Regulation (Article 20) and the proposed recast (Article 21), information related to victims of crime can be accessed by the law enforcement authorities under the same conditions as that of suspects and perpetrators, and information related to children under the same conditions as that of adults. Differentiation could be introduced in parallel with the planned adjustment of storage periods in Article 17 of the proposal.

---

[83] European Data Protection Supervisor (2012), Opinion of the European Data Protection Supervisor on the amended 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 [.../...] [.....] (Recast version), 5 September 2012, paras. 58 and 59.

FRA Opinion 14

The principle of proportionality enshrined in Article 52 (1) of the Charter, as interpreted by the Court of Justice of the EU, requires that access to personal data for law enforcement purposes is subject to adequate safeguards and that the retention of the data reflects its law enforcement relevance.

Information contained in Eurodac is collected without any evidence suggesting a link to terrorism or other serious crime, and pertains to a significant extent to persons in a vulnerable situation. In the absence of the assessment envisaged under Article 40 of Eurodac Regulation (EU) No. 603/2013, the key principles of the current model of law enforcement access to Eurodac reflected in Articles 21 and 22 of the proposed recast – in particular the clear purpose limitation and the hit/no hit access based on biometric features only – need to remain in place for access of Member States' law enforcement agencies as well as Europol.

Differentiation between the periods for which law enforcement access is possible should take into account the nature of the data and reflect the vulnerable situation of applicants for international protection, in particular the need to avoid that sensitive data are transferred to third countries. Possible future mechanisms to facilitate the interoperability of EU large-scale IT-systems should take into account the need to retain the safeguards specific for each system.

TK-05-16-102-EN-N

ISBN: 978-92-9491-577-1
doi: 10.2811/3878

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