

Transforming Eurodac from 2016 to the New Pact

From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration

■ Author

Dr Niovi Vavoula

Lecturer in Migration and Security
at the School of Law of Queen Mary
University of London

ECRE WORKING PAPER **13**

2020



ecre

European Council
on Refugees and Exiles

TABLE OF CONTENTS

1. Introduction	3
2. Eurodac: The Digital Sidekick of the Dublin System	4
2.1 The Asylum-Related Functions of Eurodac	4
2.2 Law Enforcement Access to Eurodac Data	7
3. The Legal Landscape of Europe-Wide Information Systems in the area of freedom, security and justice (AFSJ)	8
3.1 Schengen Information System (SIS)	8
3.2 Visa Information System (VIS)	8
3.3 Entry/Exit System (EES)	9
3.4 European Travel Information and Authorisation System (ETIAS)	9
3.5 European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)	9
3.6 From Independent Systems to Interoperability	10
4. The 2016 Recast Eurodac Proposal	10
4.1 The Transformation of Eurodac into a Tool for Migration Purposes	11
4.2 The Interinstitutional Negotiations	13
4.3 Fundamental Rights Assessment	15
4.3.1 Widening of Purposes Without Clarity and Demonstrated Necessity	15
4.3.2 Undifferentiated Treatment Disregards the Potential Vulnerability	16
4.3.3 Concerns regarding the capturing of biometric data of children	16
4.3.4 Capturing of Data of Third-Country Nationals who have not yet entered the EU	17
4.3.5 Rationale for Including Additional Categories of Personal Data Unclear and Unsatisfying	17
4.3.6 Disproportionate Retention Period of Personal Data	18
4.3.7 Potential of International Transfers of Stored Data to Third Parties	19
4.3.8 Right to Information Improved	19
4.3.9 Removal of Important Safeguards as Regards Law Enforcement Access	20
5. The 2020 Eurodac Proposal	20
5.1 The Proposed Amendments	21
5.1.1 Counting Applicants for International Protection in Addition to Counting Applications	21
5.1.2. Cross-System Statistical Data	22
5.1.3 A New Category for Persons Disembarked Following a Search and Rescue (SAR) Operation and Consistency with the Proposal for a Regulation on Asylum and Migration	22
5.1.4 Consistency with the Proposal for a Screening Regulation	23
5.1.5 New Categories of Personal Data	23
5.1.6 Consequential Amendments	24
5.2 Fundamental Rights Assessment	25
5.2.1 Interlinking of Eurodac Records: Impact on the Rights to Respect for Private Life and Protection of Personal Data	25
5.2.2 Re-Categorisation of Persons Disembarked Following SAR Operations: Which Safeguards for Vulnerable Applicants?	26
5.2.3. Overemphasis on the Production of Statistical Data	27
5.2.4. Adding a Security Flag: Long Lasting Impact on the Individual	28
5.2.5 Supervision	29
5.2.6 Consequential Amendments	29
6. Concluding Remarks - Recommendations	29

1. INTRODUCTION

Eurodac, which stands for European Dactyloscopy, is an EU-wide information system that primarily processes the fingerprints of asylum seekers and certain categories of irregular migrants. Operational since 2003, Eurodac constitutes the EU's first experiment with biometric identifiers and was designed to assist in the implementation of the Dublin system for the determination of the Member State responsible for examining an application for international protection.¹ Eurodac is thus an important – yet relatively underexplored – tool of the Common European Asylum System (CEAS). The current legal basis of Eurodac is Regulation 603/2013 (recast Eurodac Regulation),² which entered into force in July 2015. The recast Eurodac Regulation replaced Regulation 2725/2000³ to enable law enforcement authorities and Europol to access under specific conditions Eurodac fingerprints for the purpose of preventing, detecting and investigating terrorist offences and other serious crimes.

Eurodac forms part of a complex network of centralised Europe-wide information systems established in the EU Area of Freedom, Security and Justice (AFSJ), which comprises of six information systems. Three are already operational – namely the Schengen Information System (SIS II), Visa Information System (VIS) and Eurodac – and three are forthcoming – the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN). These databases serve a number of often overlapping purposes ranging from border management, tackling irregular migration, facilitating returns and law enforcement. Furthermore, in the framework of interoperability information systems will “speak” to each other (there will be communication between the databases), enabling the aggregation of personal data from different sources.

On 4 May 2016, the Commission adopted a recast Eurodac proposal⁴ in the framework of revising the CEAS-related legal instruments.⁵ The proposal essentially detached Eurodac from its asylum framework and re-packaged it as a system pursuing “wider immigration purposes”.⁶ The negotiations on that

1 Regulation 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 (recast) [2013] OJ L180/31 (Dublin III Regulation).

2 Regulation 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 States responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) [2013] OJ L180/1 (recast Eurodac Regulation).

3 Regulation 2725/2000 of 11 December 2000 concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316/1, supplemented by Regulation 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No. 2725/2000 concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention [2002] OJ L62/1.

4 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 persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (recast)’ COM (2016) 272 final (2016 Eurodac Proposal).

5 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)’ COM (2016) 270 final; ‘Proposal for a Regulation of the European Parliament and of the Council 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 and amending Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents’ COM(2016) 466 final; ‘Proposal for a Regulation of the European Parliament and of the Council establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU’ COM(2016) 467 final; ‘Proposal for a Directive of the European Parliament and of the Council laying down standards for the reception of applicants for international protection’ COM(2016) 465 final; ‘Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010’ COM(2016) 271 final; Commission, ‘Proposal for a Regulation of the European Parliament and of the Council establishing a Union Resettlement Framework and amending Regulation (EU) No 516/2014 of the European Parliament and the Council’ COM(2016) 468 final.

6 Commission, ‘2016 Eurodac Proposal’, 6.

proposal led to an interinstitutional agreement in mid-2018 between the co-legislators. However, in view of the package approach to CEAS and the significant difficulties in reaching agreement on other dossiers, particularly the Dublin IV Regulation, the negotiations were halted. On 23 September 2020, the Commission proposed further amendments to the Eurodac regime⁷ within the framework of the New Pact on Migration and Asylum. The amended proposal prescribes several amendments to the functionalities of Eurodac both in the framework of CEAS and migration control and in an interoperable environment, whilst taking into account the 2018 interinstitutional agreement between the Council and the Parliament.

Against this background, the aim of this paper is to take stock of the forthcoming changes in the Eurodac legal framework, both those arising from the 2016 Proposal as well as those that emerged during the interinstitutional negotiations on that proposal, and then to analyse the fundamental rights implications of the amended Eurodac proposal of September 2020. The analysis is focused on the impact of the proposal on the rights to respect for private life (Article 7 of the EU Charter of Fundamental Rights), protection of personal data (Article 8 of the Charter), the rights of the child (Article 24 of the Charter), and the right to asylum (Article 18 of the Charter). The paper aims to provide a framework to inform policy-making.

To that end, this paper first provides a concise overview of the current Eurodac rules, as envisaged in the recast Eurodac Regulation (Section 2). Then, Eurodac is situated within the broader legal framework of EU-wide information systems in the AFSJ (Section 3), so as to provide the necessary contextual framework within which the Eurodac reforms are placed. Section 4 analyses the 2016 proposal, including the changes flowing from the negotiating process. Section 5 examines the proposed reforms to Eurodac as laid down in the 2020 proposal, in the light of the protection of fundamental rights. A conclusion summarises the findings of the research and provides for a series of policy recommendations.

2. EURODAC: THE DIGITAL SIDEKICK OF THE DUBLIN SYSTEM

Eurodac has been intrinsically linked to the operation of the Dublin system, the allocation mechanism to identify the Member State responsible for examining a specific asylum claim through an array of hierarchical criteria.⁸ This section provides an outline of the current functions of the system, both as the digital sidekick of Dublin and its ancillary objective to enable consultation of Eurodac fingerprints for law enforcement purposes.

2.1 The Asylum-Related Functions of Eurodac

According to Article 1 of the recast Eurodac Regulation, the primary purpose of the database is to:

assist in determining which Member State is to be responsible pursuant to Regulation (EU) No 604/2013 for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No 604/2013.

In order to track onward movements of asylum seekers in the EU, the recast Eurodac Regulation obliges Member States to promptly collect a full set of fingerprints from every applicant for international protection over the age of 14 when they apply for international protection.⁹ The collected fingerprints must be transmitted for storage to the Central Unit, a central database, where they are compared with fingerprints that have already been transmitted and stored by other participating countries.¹⁰ Eurodac is equipped with an Automated Fingerprint Identification System (AFIS) and functions on a hit/no hit basis, meaning

7 Commission, 'Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], 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 and amending Regulations (EU) 2018/1240 and (EU) 2019/818\ COM(2020) 614 final (2020 Eurodac Proposal).

8 From an administrative perspective, by organising the joint gathering of information by the Member States, Eurodac constitutes a prime example of a composite procedure, whereby the administrative procedure of allocating the responsible Member State in accordance with the Dublin rules is supported by information transferred to it by other Member States (horizontal cooperation) and assisted by an EU agency, eu-LISA (vertical cooperation). See Niovi Vavoula, 'Between Gaps in Judicial Protection and Interstate Trust: Information Sharing in the Dublin System and Remedies for Asylum Seekers' (German Law Journal, forthcoming 2021).

9 Recast Eurodac Regulation, art 9(1).

10 Ibid art 9(3). In cases of non-compliance with the 72-hour time frame see Article 9(2).

that the transmitted data are automatically checked against other stored fingerprints and in case of a match (hit), a notification is given.¹¹ If a Eurodac check reveals that the fingerprints have already been recorded in another Member State, the latter could be requested to take back of the asylum applicant on the basis of Dublin rules.

Furthermore, Member States are under the obligation to collect the fingerprints of all third-country nationals apprehended “in connection with the irregular crossing by land, sea or air of the Member State”¹² and transmit them to the Central Unit so that they can be compared in the future against fingerprints that may be subsequently collected from applicants for international protection.¹³ Therefore, the fingerprints of persons apprehended irregularly crossing the external border must neither be compared against the fingerprint data previously taken from other irregular border-crossers and asylum applicants nor with that of irregular border-crossers that are subsequently collected and transmitted.

For example, if a third-country national is found irregularly entering Greece, his/her fingerprints will be collected and stored in Eurodac as an irregular border-crosser. If that person then travels to France and he/she applies for international protection there, the French authorities will collect his/her fingerprints as an applicant for international protection and these will be compared against fingerprints in Eurodac. Through that comparison, the French authorities will be able to determine that the applicant has entered through Greece and could apply the “first country of entry” criterion in the Dublin III Regulation. In addition, as regards third-country nationals found “illegally staying” on national territory, their fingerprints may be collected and checked against Eurodac records to determine whether they have previously applied for international protection in another Member State.¹⁴ However, neither Member State is obliged to undertake the procedure, nor would that data have to be stored within the system.

Apart from a full set of fingerprints, Eurodac stores limited information on the sex of asylum seekers and irregular border crossers, the date of registration and transmission of fingerprints to the Central Unit and the Member State of origin.¹⁵ The person’s name, nationality or date of birth are not included and, thus, the individual is defined by no more than their fingerprints.¹⁶ In cases where a hit leads to the transfer of an applicant to another Member State pursuant to the Dublin rules, the receiving State must insert the date of arrival in the receiving State.¹⁷ That said, additional data are stored in national databases, in accordance with national law.

Each set of data on asylum applicants is stored for a period of ten years from the date on which the fingerprints are collected.¹⁸ If, in the meantime, an asylum seeker is recognised as a refugee or beneficiary of subsidiary protection, the data are “marked”, which means that in the record it is indicated that the person concerned is a beneficiary of international protection and the fingerprints may be accessed for law enforcement purposes for three years, before they are “blocked” until their erasure; upon blocking, a “hit” is not to be transmitted.¹⁹ Data are erased upon expiry of the retention period or in the case that an asylum seeker acquires the citizenship of any Member State.²⁰ As for the records on irregular border crossers, the retention period is 18 months,²¹ given that the Dublin II Regulation reduced the time period

11 Ibid art 9(5).

12 This concept is controversially extended to cases involving third-country nationals ‘apprehended beyond the external border’ where they are still en route and there is no doubt that they crossed the external border irregularly. See Council, Document 12314/00 ADD 1 (15 November 2000). As Busch has observed, ‘the obligation to take fingerprints [...] is not limited to the external border itself’. Nicholas Busch, ‘EU Law-making after Amsterdam: The Example of Eurodac’ (Fortress Europe Circular Letter, December 1999) <http://www.fecl.org/circular/5901.htm> accessed 31 December 2020.

13 Recast Eurodac Regulation, art 15(1). For an analysis of the Dublin-related functions of Eurodac see Irma van der Ploeg, ‘The Illegal Body: “Eurodac” and the Politics of Biometric Identification’ (1999) 1 *Ethics and Information Technology* 295; Evelien Brouwer, ‘Eurodac: Its Limitations and Temptations’ (2002) 4 *European Journal of Migration and Law* 231; Jonathan Aus, ‘Supranational Governance in an “Area of Freedom, Security and Justice”: Eurodac and the Politics of Biometric Control’ (2003) University of Sussex: Sussex European Institute Working Paper No 72, available at: <https://bit.ly/3bSO6oi> , accessed 31 December 2020; Jonathan Aus, ‘Eurodac: A Solution Looking for a Problem?’ (2006) 10 *European Integration online Papers*.

14 Ibid art 17.

15 Ibid arts 11 and 14(2).

16 Elspeth Guild, ‘Unreadable Papers? The EU’s First Experiences with Biometrics: Examining Eurodac and the EU’s Borders’ in Juliet Lodge (ed), *Are You Who You Say You Are? The EU and Biometric Borders* (Wolf Legal Publishers 2007) 32.

17 Recast Eurodac Regulation, arts 10(a) - (b) and 11. Similarly, if the individual has left the EU territory, this must also be indicated in the system. See arts 10(c) – (d).

18 Ibid art 12.

19 Ibid art 18(2).

20 Ibid art 7.

21 Ibid art 10.

for which a Member State is responsible for dealing with an asylum application to one year.²² Those data may be erased early if the person is issued a residence permit, leaves the EU or acquires EU citizenship.²³ Transfers of personal data to the authorities of any third country, international organisation or private entity established in or outside the EU are prohibited.²⁴

When there is a hit with existing records, Eurodac data are transferred through DubliNet, an electronic communication network set up by the Dublin III Regulation,²⁵ enabling information sharing between the national authorities dealing with asylum applications. The two involved Member States may exchange personal data other than the limited dataset stored in Eurodac through DubliNet in accordance with Article 34 of the Dublin III Regulation. Thus, it must be noted that although Eurodac fingerprinting does not determine the identity of a person *per se*, it does contribute to their identification because a link may be established between an asylum applicant and a past Eurodac entry, which is verifiable through information sharing between the state that conducts the check and the state of past Eurodac entry.²⁶ Article 1(3) of the Regulation allows the Member State using the system to cross-check the Eurodac fingerprints against other databases established under national law, thus leading to the identification of the person. As a result, Eurodac operates as a *de facto* quasi-identification tool, though strictly speaking, identification does not currently feature among the objectives of the system.

As regards individual rights, the person concerned must be informed by the Member State doing the fingerprinting in writing, and where necessary orally, in a language that they understand or are reasonably supposed to understand of the identity of the data controller; the purpose for which the data would be processed; the recipients of such data; the obligation to provide their fingerprints; and the existence of rights to access and rectification of their data.²⁷ If the person fingerprinted is a minor, the information must be provided in an age-appropriate manner.²⁸ Furthermore, rights of correction and erasure are foreseen, for which responsibility lies with the Member State that transmitted the data.²⁹ Third-country nationals or stateless persons are entitled to bring an action or complaint before the competent authorities or national courts, concerning the data relating to him or her recorded in the Central System in order to exercise their rights.

Finally, supervision of the lawfulness of the processing by national authorities is entrusted on the one hand to national supervisory authorities³⁰ and the supervision of EU institutions, *in casu* eu-LISA, is bestowed on the European Data Protection Supervisor (EDPS).³¹ The latter shall ensure that an audit of eu-LISA's personal data processing activities is carried out at least once every three years and a corresponding report should reach the European Parliament, Council, the Commission, eu-LISA and the national data protection authorities.³² As foreseen in Article 32 of the recast Eurodac Regulation, the two branches meet in the framework of the Eurodac Supervision Coordination Group, which establishes vertical cooperation national supervisory authorities and the EDPS.

On 20 July 2015, the recast Eurodac Regulation came into force. Compared to the other large-scale information systems, Eurodac is the most widely operational database functioning in 32 European countries; this includes the United Kingdom and Ireland. Norway, Iceland, Switzerland, Liechtenstein also participate as Dublin Associate States.³³ According to the latest statistics, by the end of 2019, 5,690,524 fingerprint data sets were stored in the Eurodac central system, 97% of which concerned applicants for international protection. Furthermore, Eurodac processed 916,536 transactions, out of which 592,691

22 Regulation 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national [2003] OJ L50/1, art 12. This rule is maintained under Dublin III Regulation, art 13(1).

23 Recast Eurodac Regulation, art 10(2).

24 *Ibid* art 35(1).

25 Dublin III Regulation, art 18.

26 EU Fundamental Rights Agency (FRA), 'Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac' (21 October 2015) 3.

27 Recast Eurodac Regulation, art 29(1). A common leaflet must be drawn up in the respect. See Article 29(3).

28 *Ibid* art 29(2).

29 *Ibid* art 29(5) – (8).

30 *Ibid* art 30.

31 *Ibid* art 31.

32 *Ibid* art 31(2).

33 For the measures adopted see Steve Peers and others, *EU Immigration and Asylum Law* (2nd edn, Brill 2015) 20.

were data from asylum seekers (Category 1), 111,761 in relation to irregular border-crossers (Category 2) and 211,635 transactions on searches for irregular stays in Member States (Category 3).³⁴ The prime users of Eurodac are Germany, France and Greece.³⁵

2.2 Law Enforcement Access to Eurodac Data

The primary aim of the recast Eurodac Regulation has been to open up the system to national authorities and Europol for law enforcement purposes. As a result, a fundamental change brought about was the addition of an ancillary objective to the system to allow consultation of Eurodac fingerprints by law enforcement authorities, excluding intelligence services,³⁶ and Europol for the purposes of preventing, detecting or investigating terrorist offences and serious crimes.³⁷ As a result, Eurodac has ceased to serve a unitary objective. If a designated authority and Europol wish to request comparison of fingerprint data with those already stored in Eurodac, they must follow a specific three-layered procedure.³⁸ A national designated authority must submit a reasoned electronic request to a verifying authority.³⁹ The latter must verify that three conditions are fulfilled, namely:

- a. that national fingerprint databases, as well as the AFIS of other Member States pursuant to Decision 2008/615/JHA (Prüm Decision)⁴⁰ and VIS have been consulted, and that such consultation was futile;
- b. the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences;
- c. in a specific case and there must be reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.⁴¹

After verification that the conditions for the request are met, the National Access Point will process the request transmitted by the verifying authority to the Eurodac Central System.⁴² Law enforcement authorities conduct searches of Eurodac based on latent fingerprints, that is fingerprints left on a surface which was touched by an individual and may be found in a crime scene.⁴³ Fingerprints of beneficiaries of international protection are marked for three years. This means that these data remain at the disposal of national authorities for both asylum and law enforcement purposes and, upon the expiry of the three-year period, they are blocked until their erasure.⁴⁴

34 eu-LISA, 'Eurodac Annual Report 2019' (July 2020) 12.

35 Ibid 13.

36 Recast Eurodac Regulation, 5(1).

37 For an analysis see Niovi Vavoula, 'The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015). Terrorist crimes correspond or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA, as amended by Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.. Serious crimes are specified in Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States [2002] OJ L190/1, art 2(2).

38 Recast Eurodac Regulation, art 19.

39 This body is a single authority or a unit of such an authority among the bodies responsible for the prevention, detection or investigation of terrorist offences and other serious crimes. Furthermore, in accordance with Recital 30 of the Regulation, the designated and verifying authority can be within the same organisation, however acting independent without receiving instructions.

40 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 [2008] OJ L210/1.

41 Recast Eurodac Regulation, art 20(1).

42 Ibid art 19(2).

43 As mentioned in Recital 14 of the recast Eurodac Regulation, the use of latent fingerprints is a 'fundamental facility for police cooperation'.

44 Recast Eurodac Regulation, art 18.

3. THE LEGAL LANDSCAPE OF EUROPE-WIDE INFORMATION SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE (AFSJ)

In light of the changes in the legal framework of Eurodac, as examined below, it is essential to provide a concise overview of the elaborate network of Europe-wide information systems, some of which are currently operational (SIS, VIS), whereas others are still under development (EES, ETIAS, ECRIS-TCN).⁴⁵ All information systems are operationally managed by the EU agency eu-LISA.

3.1 Schengen Information System (SIS)

Operational since 1995, the overarching purpose of SIS is to ensure a high level of security in the Schengen area by facilitating both border control and police investigations. To these ends, SIS registers alerts on various categories of persons and objects. In connection with each alert, the SIS initially stored basic alphanumeric information – such as name, nationality, the type of alert and any specific objective physical characteristics.⁴⁶ However, the pressing need to develop a second generation SIS (SIS II) so as to accommodate the expanded EU membership after the 2004 enlargement was seen as an opportunity to insert new functionalities into the system.⁴⁷ Major shifts have been the possibility of interlinking alerts that are inserted under different legal bases⁴⁸ and the storage of biometric identifiers (photographs and fingerprints) within the system.⁴⁹ In 2018, the SIS legal framework underwent another revision primarily with a view to adding certain categories of alerts.⁵⁰ According to the current rules, SIS stores alerts on persons wanted for arrest and extradition,⁵¹ missing persons, or vulnerable persons who need to be prevented from travelling,⁵² persons sought to assist with a judicial procedure,⁵³ persons or objects subject to discreet, inquiry or specific checks,⁵⁴ objects sought for the purpose of seizure or their use as evidence in criminal proceedings,⁵⁵ and unknown wanted persons.⁵⁶ In addition, the SIS stores alerts on third-country nationals subject to return procedures, which is also a new category of alerts,⁵⁷ or to be refused entry or stay in the Schengen area. In practice, alerts on third-country nationals dominate the system.⁵⁸

3.2 Visa Information System (VIS)

A post 9/11 initiative, VIS stores a wide range of personal data (both biographical and biometric) on individuals applying for short-stay (Schengen) visas. VIS was set up by a series of instruments: Decision

45 For an overview see Niovi Vavoula, 'The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Data Protection' (2020) 45(3) *European Law Review* 348.

46 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19 (CISA), art 94..

47 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) [2006] OJ L381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63.

48 Regulation 1986/2006, art 37; Decision 2007/533/JHA art 52.

49 Regulation 1986/2006, art 22; Decision 2007/533/JHA, art 22.

50 Regulation 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1; Regulation 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14; Regulation 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56.

51 Regulation 2018/1862, arts 26-31.

52 *Ibid* arts 32-33.

53 *Ibid* arts 34-35.

54 *Ibid* arts 36-37.

55 *Ibid* arts 38-39.

56 *Ibid* arts 40-41.

57 Regulation 2018/1860, art 3.

58 Regulation 2018/1861, art 24.

2004/512/EC,⁵⁹ Regulation 767/2008⁶⁰ governing the use of the system for border control purposes, and Council Decision 2008/633/JHA⁶¹ prescribing the modalities by which visa data are consulted by law enforcement authorities and Europol. VIS is also a multi-purpose tool aimed at improving the implementation of the common visa policy, but seven sub-purposes are envisaged, including the fight against fraud and visa shopping and the contribution to the prevention of threats to Member States' internal security. At the timing of writing, the co-legislators have reached agreement on the revised VIS legal framework,⁶² which extends the scope of the system to long-term visa holders, as well as holders of residence permits and residence cards, and lowers the threshold age for fingerprinting (six years).

3.3 Entry/Exit System (EES)

As regards information systems in the pipeline, Regulation 2017/2226 provides for the establishment of EES that will register the border crossings, both at entry and exit, of all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.⁶³ EES is a multi-purpose tool: it aims to enhance the efficiency and automation of border checks, assist in the identification of irregular migrants and overstayers, combat identity fraud and misuse of travel documents, and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.

3.4 European Travel Information and Authorisation System (ETIAS)

Pursuant to Regulation 2018/1240, ETIAS is also to be established, requiring all visa-exempt travellers to obtain authorisation prior to their departure through an online application in which they must disclose a series of personal data including biographical data, travel arrangements, home and email address, phone number, level of education and current occupation.⁶⁴ ETIAS applicants will be pre-vetted on the basis of background cross-checks against information systems for immigration control or law enforcement,⁶⁵ screening rules enabling profiling on the basis of risk indicators,⁶⁶ and a dedicated ETIAS watchlist.⁶⁷

3.5 European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)

The latest addition to the EU information system family is the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).⁶⁸ It emerged as a necessity in the law enforcement context because, in order to obtain complete information on previous convictions of third-country nationals, the requesting Member States were obliged to send "blanket requests" to all Member States, thus creating a heavy administrative burden.⁶⁹ The ECRIS-TCN will be a centralised system for the exchange of criminal records on convicted third-country nationals and stateless persons. The ECRIS-TCN is meant to complement the already existing, decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged among Member States.

59 Council Decision 2004/512/EC establishing the Visa Information System (VIS) [2004] OJ L213/5.

60 Regulation (EC) 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas [2008] OJ L218/60, as amended by Regulation (EC) 810/2009 [2009] OJ L243/1 (VIS Regulation).

61 Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences [2008] OJ L218/129.

62 COM(2018) 302 final.

63 Regulation 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L32720.

64 Regulation 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L61/1.

65 Ibid art 20.

66 Ibid art 33.

67 Ibid art 34.

68 Regulation (EU) 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135/1 (ECRIS-TCN Regulation); Directive 2019/884 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA [2019] OJ L151/143.

69 Ibid recital 6.

3.6 From Independent Systems to Interoperability

SIS, VIS and Eurodac were originally envisaged to operate independently, without the possibility of interacting with one another. Progressively, the need has emerged to provide technical and legal solutions that would enable information systems to complement and interact with each other. To that end, the Interoperability Regulations 2019/817 and 2019/818 adopted on 20 May 2019 prescribe four main components to be implemented: a European Search Portal (ESP), a shared Biometric Matching Service (BMS), a Common Identity Repository (CIR), and a Multiple Identity Detector (MID).⁷⁰

The ESP will enable competent authorities to simultaneously query the underlying systems (described above) and the combined results will be displayed on a single screen. Even though the screen will indicate in which EU information systems the information is held, access rights should remain unaltered. The BMS will generate and store templates from all biometric data recorded in SIS, VIS, Eurodac, EES and ECRIS-TCN. CIR will store an individual file for each person registered in the systems, containing both biometric and biographical data, as well as a reference indicating the system from which the data were retrieved. CIR's main objectives are to facilitate identity checks of third-country nationals,⁷¹ assist in the detection of individuals with multiple identities, and streamline law enforcement access. The MID will use the alphanumeric data stored in CIR and SIS II to detect multiple identities. The purpose of these components is to allow for more efficient checks at external borders, improve detection of multiple identities, and help prevent and combat irregular migration.⁷² Interoperability between EES and VIS – as both systems will record data on visa applicants – is already envisaged in the EES and ETIAS Regulations.⁷³

4. THE 2016 RECAST EURODAC PROPOSAL

At the time when the recast Eurodac Regulation came into effect, the arrivals of refugees and migrants significantly increased and certain Member States became overwhelmed with fingerprinting those that arrived at the external borders and further transited through the EU en route to their destination.⁷⁴ Failure to comply with their obligations under the Eurodac Regulation, particularly in relation to the obligation to effectively fingerprint asylum seekers and irregular entrants and transmit the relevant data to the Central System within 72 hours, became a frequent phenomenon attributed to infrastructure deficiencies or unwillingness of State authorities to take responsibility.⁷⁵ In addition, instances of a lack of cooperation in the registration process were observed, whereby particularly Eritreans and Syrians refused to have their fingerprints collected and stored.

In its European Agenda on Migration of 2015, the Commission highlighted that “Member States must [...] implement fully the rules on taking migrants’ fingerprints at the borders”.⁷⁶ In that respect, it provided guidelines to facilitate systematic fingerprinting⁷⁷ and contemplated the collection of other biometric

70 Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L135/27; Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L135/85 (Interoperability Regulations).

71 Ibid art 20. For an analysis see Niovi Vavoula, “Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?” (2020) 26(1) European Public Law 131.

72 Interoperability Regulations, art 2(1).

73 EES Regulation, art 8; ETIAS Regulation art 11.

74 For an overview see Parliament, ‘Fingerprinting migrants: Eurodac Regulation’ (PE 571.346, 2015).

75 ‘More than a third of migrants not fingerprinted, officials say’ (eKathimerini, 20 August 2015), available at: <https://bit.ly/3p2Hd7u>, accessed 31 December 2020. See European Migration Network (EMN), ‘Ad-hoc query on Eurodac fingerprinting’ (2014). In October 2015, the Commission sent administrative letters to these member States but since the concerns were not effectively addressed, in December 2015, it sent Letters of Formal Notice them urging them to correctly implement the Regulation. See Commission, ‘Implementing the Common European Asylum System: Commission escalates 8 infringement proceedings’ (10 December 2015), available at: <https://bit.ly/2M7ffZU>, accessed 31 December 2020.

76 COM(2015) 240 final, 13.

77 Commission, ‘Implementation of the Eurodac Regulation as regards the obligation to take fingerprints’ (Staff Working Document) COM (2015) 150 final. Key in the Commission’s approach is to provide for a gradation of measures targeting migrants and asylum seekers, commencing with explaining the process, possibly detain them and then use coercion. See also, EMN, ‘Ad-Hoc Query on EURODAC Fingerprinting’ (2014), available at: <https://bit.ly/2LJ7Joh>, accessed 31 December 2020.

identifiers, particularly facial images. Furthermore, Member States that are not situated at the EU periphery wanted to be able to store and compare information on irregular migrants that were found irregularly staying on their territory, particularly when the people in question did not seek asylum – in other words to extend the reach of Eurodac so that the information on irregular migrants would not be used solely for asylum-related purposes. These challenges were coupled with the low number of completed returns of irregular migrants pursuant to the Return Directive.⁷⁸ With less than 40% of the irregular migrants that were ordered to leave the EU actually departing,⁷⁹ calls to increase the effectiveness of the EU return system proliferated, including through the enhancement of information sharing to enforce return.⁸⁰

Against this backdrop, on 4 May 2016, the Commission tabled an amended proposal on Eurodac,⁸¹ which formed part of the broad reform of CEAS. The section below outlines the key changes to Eurodac stemming from that proposal, followed by an overview of the additional reforms agreed by the co-legislators so as to provide the full picture of how Eurodac is reconfigured. ECRE has published comments on the proposal, thus the section below should be viewed in conjunction with that analysis.⁸²

4.1 The Transformation of Eurodac into a Tool for Migration Purposes

The 2016 proposal marked a landmark change in Eurodac's purpose from a system ensuring the effective implementation of the Dublin mechanism to an instrument serving wider immigration purposes, including the return of irregular migrants. This approach is based on a deflection continuum, whereby collection of personal data must take place as early as possible, as the expulsion and non-protection of third-country nationals is actively sought with pre-emptive measures taken. In addition to the existing objectives of the system outlined above, the proposal foresaw that Eurodac would:

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.⁸³

The thinking is for Eurodac to be useful where Member States face problems in identifying irregular migrants found on their territory who use deceptive means to avoid identification and to frustrate the procedures for re-documentation in view of their return and readmission.⁸⁴ By comparing their data with those already stored in Eurodac, the database could thus facilitate identification and re-documentation for the purposes of return and readmission.

These changes to Eurodac result in an expansion of the personal scope of the system. the addition of categories of personal data to be collected and stored, and an increase in the retention periods. In particular, on top of a full set of fingerprints, Member States will be obliged to capture and transmit a facial image in relation to all three categories falling within the personal scope of Eurodac.⁸⁵ Thus, information on persons who are found irregularly present will be centrally stored. The proposal has given Member States the discretion to impose administrative sanctions on those individuals who refuse to comply with the registration procedure, including the possibility of detention “as a means of last resort in order to determine or verify a third-country national's identity”.⁸⁶

The age threshold for children has been significantly reduced to the age of six.⁸⁷ In the case of Eurodac,

78 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 [2008] OJ L348/98.

79 COM(2015) 453 final, 1.

80 Ibid 6-7.

81 Commission, '2016 Eurodac Proposal' (n 4).

82 ECRE, 'ECRE Comments on the Commission Proposal to recast the Eurodac Regulation COM(2016) 272' (2016).

83 Ibid art 1(1)(b).

84 Ibid recital 12.

85 Ibid art 2(1). These fingerprints may be collected and transmitted at the discretion of Member States by members of the European Border Guard Teams or Member States asylum experts. See art 10(3).

86 Ibid art 2(3).

87 Ibid art 2(2). This policy choice has been informed by Fingerprint Recognition for Children, 'Technical report by the Joint Research Centre' (2013), available at: <https://bit.ly/3sJzWMZ>, accessed 31 December 2020.

this change has been branded as a means to assist in the identification of children in cases where they are separated from their families or abscond from care institutions or child social services.⁸⁸ The proposal is mindful of children's rights by requiring that the capturing of fingerprints and facial images should take place in a "child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and facial images".⁸⁹ The child would 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 children and they would be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image are taken. The dignity and physical integrity of the child during the fingerprinting procedure and when capturing a facial image should be respected.⁹⁰

The categories of data held in Eurodac have also been considerably expanded with Member States required to store additional information as follows. In relation to asylum seekers the data set recorded shall include: a) facial image, to mitigate the risk of damaged fingertips; b) name (or known alias); c) nationality; d) place and date of birth; e) information on travel or identity document; f) asylum application number; g) allocated Member State; h) where applicable, the date of transfer to the allocated Member State.⁹¹ In relation to irregular border crossers and irregular residents, the system will store the elements under (a) – (d), as described above, as well as the date on which the person concerned left or was removed from EU territory.⁹²

To ensure the accuracy of a hit, both types of biometric data – fingerprints and facial images – will be automatically compared to the ones already transmitted and stored by other Member States.⁹³ Eurodac would allow the construction of patterns of irregular or secondary movements throughout the EU⁹⁴ by following the chronology of an immigration narrative from the EU periphery to the core. The 2016 proposal has allowed comparisons to be based solely on facial images, as a last resort, in circumstances where an individual's fingertips are too damaged to ensure a high level of accuracy or where the individual concerned refuses to provide fingerprints.⁹⁵ Recital 10 has further noted that where facial images could be used in combination with fingerprint data, it would allow for the reduction of fingerprints registered while enabling the same result in terms of accuracy of the identification.

The retention period for personal data of asylum seekers was left unchanged⁹⁶ "to ensure that Member States can track onward movements within the EU following a grant of international protection status where the individual concerned is not authorised to reside in another Member State".⁹⁷ The retention period of records on irregular migrants was increased to five years.⁹⁸ Irregular migrants' data will be marked when obtaining a residence permit or leaving the EU territory.⁹⁹ That marked data will be made available for comparison until their erasure at the five-year point.¹⁰⁰

With regard to the transfer of data to third countries, the proposal foresaw the transfer of data solely for the purpose of identifying and re-documenting in the process of return and readmission.¹⁰¹ Such transfer would be based on two cumulative conditions:

- a. the third-country national explicitly agrees to it and
- b. the Member State of origin gives its consent and the individual concerned has been informed that his or her personal information may be shared with the authorities of a third-country. No information on the fact that an asylum application has been lodged would be disclosed.

88 Commission, '2016 Eurodac Proposal' (n 4) explanatory memorandum, 10.

89 Ibid art 2(2).

90 Ibid.

91 Ibid art 12.

92 Ibid arts 13-14.

93 Ibid art 15(1).

94 Ibid explanatory memorandum, 13.

95 Ibid arts 16(1).

96 Ibid art 17(1)

97 Ibid explanatory memorandum, 14.

98 Ibid arts 17(2) and (3).

99 Ibid art 19(4).

100 Ibid art 19(5).

101 Ibid art 38.

As for individual rights, the proposal has significantly strengthened the right to information in various ways:

- a. it is explicitly foreseen that information should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- b. the obligation to provide information about the details of the data protection officer;
- c. the remark that the recipients or categories of recipients of personal data would be communicated;
- d. the obligation to inform the person about the retention period;
- e. and about the existence of the right to lodge a complaint with the national supervisory authority.¹⁰²

As regards the rules on law enforcement use of Eurodac data, the proposal did not alter much, however comparison of data on irregular migrants granted a residence permit can be consulted for law enforcement purposes until their deletion.¹⁰³ Furthermore, in the case of children, use for law enforcement purposes may take place in accordance with the requesting Member State's laws applicable to children and in accordance with the obligation to give primary consideration to the best interests of the child.¹⁰⁴

As a final note, the proposal has provided a detailed set of statistical data that eu-LISA will produce on the basis of information stored in Eurodac, in relation to the numbers of apprehensions and secondary movements.¹⁰⁵

4.2 The Interinstitutional Negotiations

The negotiations for on the expanded Eurodac went hand in hand with those on the whole range of the CEAS legal instruments based on the package approach to the proposals. As a text consolidating the interinstitutional agreement is not available – at least at the time of writing – this Section summarises the most important amendments on the basis of existing Council documentation.

With regard to protection of children, in order to increase the safeguards, it was added that minors would be accompanied by a [legal representative, guardian] or a person trained to safeguard the best interest of the child and his or her general well-being. Furthermore, sufficient care must be taken to ensure an adequate quality of fingerprints of the minor and to guarantee that the process is child-friendly so that the child, particularly a very young child, feels safe and can readily cooperate with the process of having his or her biometric data taken.¹⁰⁶

Eurodac has been further opened up to a category of third-country nationals which had been so far off the EU monitoring radar: persons admitted in the context of the Union Resettlement Framework, as proposed by the Commission in the CEAS legislative package of 2016,¹⁰⁷ or resettled in accordance with a national resettlement scheme. With common EU rules and procedures currently missing, resettlement has taken place since 2015 through a combination of multilateral and national schemes on a voluntary basis.¹⁰⁸ The proposal for a Union resettlement framework aimed to complement the ad hoc resettlement programmes by creating a common policy on resettlement with rules on the admission of third-country nationals, decision-making procedures, types of status to be accorded and financial support. In a partial provisional agreement reached in June 2018, it was agreed to include humanitarian admission – alongside resettlement – to the scope of the proposed Regulation. Against this backdrop, and in view of the EU role in resettling refugees solidifying, the idea emerged that Eurodac could be used to facilitate the application of the admission and resettlement rules.¹⁰⁹ Eurodac will thus store data on persons registered for the purpose of conducting an admission procedure and persons resettled in accordance with a national resettlement

102 Ibid art 30(1)

103 Ibid art 18(4).

104 Ibid recital 26.

105 Ibid art 11.

106 Council, Document 14462/16 (18 November 2016) 17.

107 Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a Union Resettlement Framework and amending Regulation (EU) No 516/2014 of the European Parliament and the Council' COM(2016) 468 final.

108 For the EU resettlement schemes see Commission 'Recommendation (EU) 2015/914 of 8 June 2015 on a European resettlement scheme' C(2015) 3560 final; 'Commission Recommendation (EU) 2017/1803 of 3 October 2017 on enhancing legal pathways for persons in need of international protection' C(2017) 6504 final.

109 Council, Document 7558/17 (28 March 2017). See Council, Document 9187/17 (16 May 2017).

scheme. The justification of this new entry was twofold: first, to establish the identity of persons in the admission or resettlement procedure; and second to reduce the risk of onward movements from the territory of the Member State to which a person has been admitted to the territory of another Member State.¹¹⁰ Through it, Member States will be enabled to check whether persons found irregularly staying have been resettled in accordance with the EU or a national resettlement scheme. This includes cases where a Member State reaches a negative conclusion on the admission because the information allows the Member States to apply the refusal grounds laid down in Article 6 of the Resettlement Regulation.¹¹¹ Whereas for individuals admitted the retention period mirrors the basic ten-year rule, for individuals not selected for admission the retention period will be three years.¹¹²

The references that the comparison of facial images without fingerprints would be a measure of last resort and the possibility to remove fingerprints due to the capturing of a facial image was deleted.¹¹³ Furthermore, the issue of whether an expert would need to verify a hit based on a comparison of facial images emerged and it was proposed that a hit would be verified by an official trained in accordance with national practice, particularly where the comparison is made with a facial image only. However, where a fingerprint and facial image comparison is carried out simultaneously and a hit result is received for both biometric data sets, Member States may check and verify the facial image result, if needed.¹¹⁴ In addition, the introduction of administrative sanctions against third-country nationals obstructing the capturing of biometric identifiers became mandatory,¹¹⁵ including the use of coercive means.¹¹⁶

Another important change involves the addition of copies of travel or identity documents, as well as other documentation (birth certificates, marriage, divorce and citizenship or driving licences) to the list of personal data stored in Eurodac. This revision was prompted by the fact that a significant number of countries of origin demand an actual copy of a passport or identity card and will not accept just a serial number and personal data.¹¹⁷ Only authenticated documents or documents the authenticity of which cannot be established should be kept in the system to aim at facilitating the identification of third-country nationals during the return process.¹¹⁸ An indication of the authenticity of each document stored would also be recorded.¹¹⁹

Finally, as regards law enforcement access to Eurodac, every safeguard in the recast Eurodac Regulation was called into question with the aim of aligning the modalities of access with those prescribed in the legal bases of other information systems, particularly VIS and EES.¹²⁰ A large majority of Member State delegations found the modalities too complex, cumbersome, time- and human resource consuming and therefore not attractive and were in favour of simplified access of law enforcement authorities to Eurodac data. This is notwithstanding the fact that at that time a number of Member States' authorities were not yet connected to the system and therefore did not have practical experience of it. Overall, in order to address the "challenge of maintaining security in an open Europe", which requires the EU to "do its utmost to help Member States protect citizens", four key changes emerged:

- a. the requirement to check VIS before a Eurodac check is deleted;¹²¹
- b. access to be allowed not only in a specific case but also in connection with specific persons;¹²²

110 Council, Document 8502/17 (28 April 2017).

111 Council, Document 6016/2018 (12 February 2018).

112 This was a particularly contentious issue with the Parliament, See Council, Document 12802/17 (6 October 2017); Council Document 15057/1/17 (1 December 2017). For revision see Council Document 14570/17 (12 December 2017) 17. See also Council, Document 6016/18 (n 111) 3.

113 Council, Document 12816/16 (5 October 2016) 7.

114 Council, Document 14710/16 (28 November 2016) 19.

115 Council, Document 12816/16 (n 113) 40.

116 Council, Document 14462/16 (18 November 2016) 39; Document 6016/18 (12 February 2018) 32.

117 Council, Document 12816/16 (28 March 2017) 56.

118 Council, Document 8502/17 (28 April 2017) 8.

119 Council, Document 9187/17 (16 May 2017).

120 Furthermore, in its Communication on stronger and smarter information systems from April 2016, the Commission had already announced that the modalities of access to Eurodac would be reconsidered with a view to providing for simplified procedures so that law enforcement access could take place more rigorously. See COM(2016) 205 final, 9.

121 Council, Document 6016/18 (n 111) 71.

122 Ibid 79-80.

- c. consultation to take place through both biometrics and alphanumeric data;¹²³ police investigators quite often do not have access to the persons they are investigating (suspected criminals or victims), for example, in cases of victims of trafficking or smuggling; and
- d. Eurodac data in respect of beneficiaries of international protection will be marked and used for law enforcement purposes until their erasure.¹²⁴

4.3 Fundamental Rights Assessment

The Eurodac reform has taken place both qualitatively, through the expansion of the personal scope and the obligation to register additional categories of data, and quantitatively, by detaching Eurodac from its original Dublin context and re-conceptualising it as a highly elaborate, multi-purpose tool.

4.3.1 Widening of Purposes Without Clarity and Demonstrated Necessity

From the perspective of the rights to respect for private life (Article 7 Charter) and protection of personal data (Article 8 Charter), the additional aims constitute a considerable deviation from the original purpose of the system. Once information is collected it can be used in a multiplicity of contexts, even without much justification, even if the individuals concerned have not been informed about the further use of their personal data beforehand. This puts pressure on the purpose limitation principle of data protection law, as set out in Article 5(1)(b) of the General Data Protection Regulation (GDPR).¹²⁵ In addition to the registration of fingerprints, applicants for international protection and irregular migrants will also have their facial image captured and recorded in the system. This process enhances the negative connotations of criminality generated by fingerprinting and deepens the surveillance of movement. The feeling of surveillance is further exacerbated by four factors: the expansion of the categories of data stored; the mandatory recording of irregularly present migrants; the lower minimum age for registration; and the extension of the retention period, all of which will magnify the size of the system.

Consequently, the revised framework transforms Eurodac from a relatively restricted database, compared to VIS and SIS for example, into a powerful tool of mass surveillance, whereby national authorities will be able to track third-country nationals whose data are recorded within the EU for as long as they remain on EU territory. This involves not only irregular migrants, whose movement is monitored with a view to removing them, but also beneficiaries of international protection, in relation to whom surveillance is aimed at confining them to where they should be according to EU rules. National authorities will be able on the basis of a hit to recreate migration routes on an unprecedented scale by processing “real-time” information.

The additional objectives of the new Eurodac, namely the control of “illegal immigration”, and “secondary movements with the Union”, and the “identification of illegally staying third-country nationals” are considered as purposes of general interest to the EU falling within implementation of the EU’s return policy and its combat against irregular migration. Nevertheless, the proposal does not clearly explain these purposes, or what constitutes “appropriate measures”, which are mentioned therein or what is the ultimate aim.¹²⁶ In that respect, that revision of Eurodac was necessary to assist in effecting returns is, at best, extremely doubtful.¹²⁷

The sole explanation provided involves the need to collect and store a facial image on top of fingerprints, which is grounded on cases where third-country nationals refuse to undergo the fingerprinting process in an attempt to bypass the Dublin rules or due to fear that their personal data will be misused. In this context, instead of reconfiguring the EU’s asylum policy more broadly in order to re-build trust with applicants for international protection, the introduction of an additional means of assigning an identity to third-country nationals was selected.

¹²³ Council, Document 15166/1/16 (2 December 2016). See also Council, Document 14858/16 (6 December 2016) 13.

¹²⁴ Council, Document 6016/18 (n 111) 67-68.

¹²⁵ Regulation 2016/679 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 [2016] OJ L119/1 (General Data Protection Regulation),

¹²⁶ The proposal referred to repatriation and return, but this reference has been removed. See EDPS, ‘Opinion 07/2016 EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)’ (21 September 2016) 7-8.

¹²⁷ On this issue see ECRE, ‘ECRE Comments on the Commission Proposal to recast the Eurodac Regulation’ (n 82).

4.3.2 Undifferentiated Treatment Disregards the Potential Vulnerability

Furthermore, the undifferentiated treatment of irregular migrants and applicants for international protection disregards the potential vulnerability of the latter group, as well as the particularities of the policies applicable to different groups of people. It creates a negative precedent, whereby asylum seekers and irregular migrants are brought together with the end result being the downgrading of embedded safeguards. This is all the more evident in the requirement to store the personal data of irregularly staying migrants, without any differentiation in cases where those individuals had entered regularly and only at a later stage overstayed their visa. Onward movements within the EU should not be treated in the same way as irregular migration,¹²⁸ given that a refugee may have valid reasons for traveling from a country that does not provide any protection to a Member State where they are safe.

4.3.3 Concerns regarding the capturing of biometric data of children

Moreover, the broadened personal scope of Eurodac to require the capturing of biometric data of children raises concerns. Even though this choice was advocated for as a means to assist in locating missing children, establishing links with family members in other Member States or prevention of exploitation, none of these objectives features in the proposal or in proposed amendments.¹²⁹ As the EDPS has mentioned, this justification “is not convincing as such” and the mere fact that some Member States have adopted this practice does not mean that such a measure is efficient, proportionate or useful.¹³⁰ The justification may have merely been an excuse to widen pre-emptive surveillance, particularly in view of the prolonged retention period by the end of which individuals would be, if not adults, at least close to adulthood. Capturing the biometrics of children poses significant challenges to the protection of their rights in accordance with the UN Convention on the Rights of the Child, due to their inherent vulnerability. Furthermore, unaccompanied minors should be considered as extremely vulnerable. It is not argued that protecting minors is not a noble purpose, at least in principle. However, as it will be shown below the limitations in use and the safeguards included are not always satisfactory, not least because the use of the data solely for the purpose of identifying relatives is not foreseen.

That said, it is contended that as regards the procedure for capturing biometric data, the proposal – and the interinstitutional agreement – incorporates increased safeguards to mitigate risks during capturing of biometric data of children by requiring the involvement of a trained official proceeding in the presence of a responsible adult, taking into account the rights of the child, including their dignity, and proscribing sanctions. In that respect, there are some points where the text could be further enhanced, first, to ensure that appropriate procedures exist in order to determine the age of the child and whether they fall within the remit of Eurodac and second, that the procedure in respect of female applicants and irregular migrants should be conducted where possible by female staff.¹³¹

International organisations including UNHCR, UNICEF, OHCHR, and IOM and civil society organisations urged the Council of the European Union, the Parliament and the Commission to exempt all children, no matter their age, from all forms of coercion in the Eurodac Regulation, to fully comply with the UN Convention on the Rights of the Child (CRC). They stated that the identification and registration of children contributes to their protection within and across borders but that this must be done in a child-sensitive manner and that the best interests of the child must be a primary consideration, in accordance with Article 3 of the CRC. They agreed with the opinion of the Fundamental Rights Agency, and guidance from the UN Committee on the Rights of the Child that collecting and using children’s data can only be justified if it pursues a clear child protection objective. Even when done with a child protection objective in mind, coercion of children in any manner or form in the context of migration-related procedures, violates children’s rights, which EU Member States have committed to respect and uphold.¹³²

128 Meijers Committee, ‘Note on the reforms of the Dublin Regulation, the Eurodac proposal and the proposal for an EU Asylum Agency (CM1609, 2016).

129 FRA, ‘The impact of the proposal for a revised Eurodac Regulation on fundamental rights - Opinion of the European Union Agency for Fundamental Rights’ (2017) 23.

130 EPDS, ‘Opinion 07/2016’ (n 126) 9.

131 FRA, ‘The impact of the proposal for a revised Eurodac Regulation on fundamental rights’ (n 128) 14-15.

132 ‘Joint Statement: Coercion of children to obtain fingerprints and facial images is never acceptable’ (Unicef, 2 March 2018), available at: <https://uni.cf/3bXYjQh>, accessed 31 December 2020.

In that respect, the Council's position did not unequivocally reject coercion in the case of children. On the one hand, it is stated that "third-country nationals or stateless persons who are deemed to be 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*".¹³³ On the other hand, it is stated that "where enrolment of biometric data is not possible from [...] vulnerable persons and from a minor due to the conditions of the fingertips or face, the authorities of that Member State shall not use sanctions to coerce the taking of biometric data".¹³⁴ However, it is then mentioned that "[a] Member State may attempt to re-take the biometric data of a minor or vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual and where it is duly justified to do so". In light of the international legal framework described above, any coercion of children must be explicitly forbidden without leaving loopholes at the national level.

4.3.4 Capturing of Data of Third-Country Nationals who have not yet entered the EU

The addition during the negotiations of persons identified for an admission procedure on humanitarian grounds and resettlement as part of EU or national schemes is part of the effort to fill informational gaps concerning the movement of third-country nationals in the EU by capturing the personal data of categories of people previously not covered by digital monitoring under EU law. Eurodac rules require Member States to transmit personal data of applicants of international protection but this procedure involves those who have already reached the EU territory. The expanded personal scope involves groups of individuals who are selected for admission from the territory of a third country, for example from the country of origin or from third countries, such as Turkey, following an assessment of their eligibility. Their inclusion within scope of Eurodac thus raises the question as to whether the capturing of data should take place before or after the arrival of the person to the EU "for security purposes". It has been noted in that respect that the:

security verification should be done on the basis of the data collected in the third country in order to minimise the risk of transferring persons who may pose a security risk to EU citizens and at the same time limit administrative burden in case the person has to be returned based on information obtained from the comparison of the biometric data.¹³⁵

This policy choice raises significant challenges to the protection of the rights to private life and protection of personal data because the capturing of a series of personal data, including two types of special categories of personal data, may take place outside the EU, in third countries where adherence with the protection of fundamental rights, including regarding biometric data, may not be safeguarded.

Another issue is how to reconcile the resettlement of individuals to national territory under national resettlement schemes with the capturing of data in an EU-wide information system. It is similar to the expansion of the scope of VIS to store personal data of long-stay visa holders and holders of residence permits and residence cards even though the issuance of such documents falls within the competence of Member States. The preoccupation with security concerns and the safeguarding of free movement in the EU are used to justify including all third-country nationals on EU territory. Finally, by including both positive and negative decisions on admission in order to allow Member States to exchange information on rejected cases, Eurodac facilitates the use of the additional – problematic – exclusion grounds from humanitarian admission or resettlement programmes.¹³⁶

4.3.5 Rationale for Including Additional Categories of Personal Data Unclear and Unsatisfying

As regards the categories of data collected, it is not clear why the system must store the categories set out, some of which pose challenges as regards the rights to respect for private life and protection of personal data.¹³⁷ In accordance with the data minimisation principle, as laid down in Article 5(1)(c) of the GDPR, the collected data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

¹³³ Council, Document 6016/2018 (n 111) 20.

¹³⁴ Ibid 33.

¹³⁵ Council, Document 6016/18 (12 February 2018) 2.

¹³⁶ ECRE, 'EU Resettlement for Protection – ECRE's Analysis of the Latest Developments in the Preparation of an EU Resettlement Framework' (2017).

¹³⁷ Steve Peers, 'The Orbanisation of EU asylum law: the latest EU asylum proposals (EU Law Analysis, 06.05.2016), available at: <https://bit.ly/3p4Bmi6>.

In the present case, the underlying rationale seems to be the alignment with other operational information systems, which is an irrelevant factor. As for the inclusion of both fingerprints and a facial image, it is inexplicable that the requirement to register an additional type of biometric data, which is a special category of personal data, has not been accompanied by a revision of the existing rules requiring the registration of a full set of fingerprints. The reference in the proposal to enable the capturing and storage of fewer fingerprints in cases when both fingerprints and a facial image have been collected did not make it into the final text.

Furthermore, concerns about the reliability of biometric data of children and ultimately the accuracy of the results, are relevant here as well, particularly in light of the long retention period, during which a person's appearance may significantly change. It is contended, however, that the cumulative effect of comparing both a facial image along with fingerprints will result in higher levels of accuracy; nonetheless, deeper surveillance of applicants of international protection and irregular migrants will take place. The reference in Article 16 of the proposal to facial recognition only occurring as a last resort where the quality of fingerprints does not allow for a comparison, or where the individual refused to comply with the fingerprinting procedure, has been deleted. In addition, with regard to children, it could also be argued that Eurodac should store family links so as to enable the reconnection between family members.¹³⁸

As for addition of coloured copies of identity, travel or other documents in the system, in principle this reform may resolve cases where Member States of origin may have proceeded to wrongful categorisation of an application for example as an adult instead of a child, so that national authorities in other Member States do not have to resort to exchange of information pursuant to Article 34 of the Dublin III Regulation, which is considered to be of administrative nature and to not have a fundamental rights dimension.¹³⁹ However, it is unclear as to whether this could not take place through bilateral information exchange of information stored in national databases following a hit.

4.3.6 Disproportionate Retention Period of Personal Data

With respect to the retention period of the personal data collected, it is striking that the rule requiring the storage of asylum seekers' personal data for 10 years has remained unaltered. As opined in a series of judgments by the European Courts, in order for an interference with the rights to respect for private life and protection of personal data arising from the collection and storage of personal data to be proportionate, the retention period should be limited on the basis of the data's potential usefulness and should remain as short as possible.¹⁴⁰ It is noteworthy that even the strong efforts of the Parliament during the negotiations with the Council to reduce the retention period were unsuccessful.¹⁴¹ However, the Parliament did manage to insert a safeguard that data on persons with long-term resident status would be deleted from the system.¹⁴²

Furthermore, it must be pointed out that a 10-year retention period in respect of children is also

138 FRA, 'The impact of the proposal for a revised Eurodac Regulation on fundamental rights' (n 131) 24.

139 In a Dutch case, an Eritrean asylum seeker who though a minor, was registered as an adult by the Italian authorities. When she applied for international protection in the Netherlands, she informed the immigration authorities (IND) that she was in fact 15. The IND, however, refused to treat her as a minor relying upon the data submitted by the Italian counterparts. As a result, the minor did not receive appropriate protection even though she corroborated her statement about her age with documents and her appearance and behaviour made clear she was at the time a minor. In its decision of 4 April 2019, the Dutch Council of State held that the State Secretary had in principle rightly assumed that the registration of the applicant as an adult has been carried out carefully so that it was up to the foreign national to demonstrate that the date of birth registered in Italy was incorrect. In the Court's view, the applicant had failed to do so; a baptism document that was submitted was not accepted as it was not an identifying document issued by the Eritrean authorities. Furthermore, as a copy of a school card did not include her place of birth, that was also not considered sufficient. Therefore, the Court found that it was correct not to doubt the date of birth registered in Italy and thus to not offer an age test. This is despite the fact that the incorrect registration of a minor's age is a common occurrence, particularly in periods of chaos when large numbers of asylum seekers arrive, but sometimes also due to miscommunication or a lack of information provided to minor asylum seekers. See ABRvS 11 April 2019, AR 2019/106, ve19001150, available at: <https://bit.ly/3bYe9un>.

140 S and Marper (2009) 48 EHRR 50; Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Ireland ECLI:EU:C:2014:238, paras 63-64.

141 Parliament, 'Report on the proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) (COM(2016)0272 – C80179/2016 – 2016/0132(COD))' (8 June 2017) 20. See Council, Documents 12802/17 (n 112); 15057/17 (n 112).

142 Council, Document 9848/18 (12 June 2018).

disproportionate; the appearance of children will change and therefore the data will cease to be of adequate quality or relevance.¹⁴³

The duration of the retention period for irregular migrants is also disproportionate to the aim pursued. According to the Commission, the aim of such collection and storage will be to use this information “to assist a Member State to re-document a third-country national for return purposes”.¹⁴⁴ Also taking into account the maximum length of detention for the purposes of return to the country of origin, the five-year retention period seems unreasonably long. Arguments related to the duration of an entry ban or the length of the retention period for other categories of third-country nationals in other databases are irrelevant as each database exists for different purposes, which in turn determine the retention period. Alignment does not serve the objectives of the database but rather the underlying and future aim of making the systems interconnected. Even if it were to be accepted that the retention period should be aligned with the duration of an entry ban, then this alignment should be with the *actual* duration of the entry ban placed upon a specific third-country national, which may be less than five years. Consequently, once an entry ban on an individual has expired, the information on this individual should be erased from Eurodac, and not only after a period of five years, which is a theoretical maximum period.¹⁴⁵

4.3.7 Potential of International Transfers of Stored Data to Third Parties

The future use of Eurodac for return purposes opens up the system to potential international transfers of stored data to third countries, international organisations and private entities. In addition to implications for the rights to respect for private life and protection of personal data, such transfers may entail violation of the prohibition of non-refoulement. It is regrettable that the two conditions for such transfers mentioned in the proposal were removed during the negotiations and that only a general reference to the GDPR is foreseen.¹⁴⁶ It must be emphasised that the countries of return will almost always be countries whose protection of personal data will not be “equivalent” to that offered at EU level. The GDPR allows transfers to such parties on the basis of adequate safeguards or derogations for specific situations. The removal of specific safeguards, for example the explicit consent of the individual concerned and of the Member State that recorded the data in Eurodac, disregards the supposed exceptional character of the transfer and may result in the transfer of personal data en masse to “safe third countries”. In addition, there are no limitations on or specifications as to the categories of personal data that may be transferred,¹⁴⁷ nor is there reference to the specific situation of minors.¹⁴⁸

4.3.8 Right to Information Improved

A positive reform involves the right to information, which has been reinforced by requiring that more extensive information will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.¹⁴⁹ Additional safeguards are included in relation to children, the right to information of whom will be safeguarded by child-oriented information. Nonetheless, the information should also be provided orally,¹⁵⁰ so that it is easier for the responsible adult to verify that the child has understood the information provided and the purposes of capturing their biometrics. In that regard, a safeguard requiring Member States to ensure that all third-country nationals or stateless persons subject to Eurodac rules have comprehended the content of the information provided is vital, as practice shows that the provision of information does not always mean that individuals have understood that information. Furthermore, the potential that personal data already stored in the system collected from individuals who have not been informed about the additional use creates an “information creep”, whereby individuals may find themselves in a return procedure based on fingerprints that have been provided prior to the enactment of the revised rules cannot be overruled.

143 FRA, “The impact of the proposal for a revised Eurodac Regulation on fundamental rights’ (n 131) 24.

144 Commission, ‘2016 Eurodac Proposal’ (n 4) explanatory memorandum, 3.

145 EDPS, ‘Opinion 07/2016’ (n 126) 10.

146 GDPR, arts 44-50.

147 EDPS, ‘Opinion 07/2016’ (n 126) 13.

148 Committee of the Regions, ‘Opinion of the European Committee of the Regions — Reform of the Common European Asylum System’ [2016] OJ C 185/91, 100-101.

149 For guidelines see FRA, ‘Right to information — Guide for authorities when taking fingerprints for EURODAC’ (2019), available at: <https://bit.ly/3qE9pOn>, 31 December 2020.

150 FRA, “The impact of the proposal for a revised Eurodac Regulation on fundamental rights’ (n 131) 20-21.

4.3.9 Removal of Important Safeguards as Regards Law Enforcement Access

Finally, it is striking that the 2016 proposal has led to proposed removal of important safeguards that made their way into the recast Eurodac Regulation following heated negotiations and based on recognition of the need for differential treatment of data collected from asylum seekers.¹⁵¹ This involves the prerequisite for prior search in VIS, the possibility to conduct searches also in connection to specific persons, and the removal of the blocking of Eurodac data in relation to beneficiaries of international protection three years after they obtained status. The simplification of the modalities of access does not justify the impact on the rights to respect for private life and protection of personal data. The changes are wrongly premised on the equation of VIS and Eurodac as centralised information systems processing personal data of third-country nationals and disregards the specificities of the personal scope and the purposes of each system. This is a misplaced approach, not least because of the vulnerabilities of asylum seekers and irregular migrants and the (in principle) voluntary character of Schengen visa applications, factors which are completely disregarded in favour of law enforcement considerations, despite the lack of evidence of the necessity of such reforms.

This approach embraces the trend of equating the different groups of third-country nationals covered by Eurodac, all of whom are considered to present a security risk irrespective of whether they are entitled to international protection. Astonishingly, no proof has been provided to justify why beneficiaries of international protection may pose a security threat three years after the recognition of their status such that their records should remain accessible for law enforcement purposes. Furthermore, the possibility to conduct searches in relation to specific persons in addition to specific cases may increase significantly the number of searches, for instance in cases where fingerprints are found at a crime scene, as there is no specification in the legislation that the person has to have been identified.

5. THE 2020 EURODAC PROPOSAL

In July 2019, a New Pact on Migration and Asylum was announced, advocating a “comprehensive approach to external borders, asylum and return systems, the Schengen area of free movement, the external dimension of migration, legal migration and integration, to promote mutual trust among Member States”.¹⁵² The New Pact builds upon the Commission CEAS proposals of 2016, as well as the proposal for a revised Return Directive adopted in 2018.¹⁵³ In what was heralded as a “fresh start on migration”,¹⁵⁴ the Pact and a first batch of legal instruments was published on 23 September 2020, comprising of five legislative proposals:

- an amended Proposal for a Eurodac Regulation, analysed below;
- an amended Proposal for Asylum Procedure;¹⁵⁵
- a Proposal for an Asylum and Migration Management Regulation;¹⁵⁶
- a Proposal for a Screening Regulation;¹⁵⁷
- a Proposal for a Crisis and Force Majeure Regulation.¹⁵⁸

151 It is recalled that no less than four legislative proposals were necessary before the Parliament agreed to this reform.

152 Commission, ‘2020 Eurodac Proposal’ (n 7) explanatory memorandum, 1.

153 Commission, ‘Proposal for a Directive of the European Parliament and of the Council on common standards and procedures in Member States for returning illegally staying third-country nationals (recast)’ COM(2018) 634 final.

154 Ibid.

155 Commission, ‘Amended proposal for a Regulation of the European Parliament and of the Council establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU’ COM(2020) 611 final.

156 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund]’ COM(2020) 610 final (Proposal for a Regulation on Asylum and Migration Management).

157 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council introducing a screening of third country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817’ COM(2020) 612 final (Proposal for a Screening Regulation).

158 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council addressing situations of crisis and force majeure in the field of migration and asylum’ COM(2020) 613 final.

It also includes a number of non-legislative initiatives.¹⁵⁹

The amended Eurodac proposal introduces new elements to the existing interinstitutional agreement between the Council and Parliament based on the 2016 proposal.

The explanatory memorandum notes that the aim of the amended proposal is to ensure consistency with the revised procedures and rules set out in the proposal for a new Regulation on Asylum and Migration Management, and the screening process laid down in the proposal for a Screening Regulation. Other objectives of the amendments are to enable the gathering of more accurate and complete data to inform policy making, as well as to adjust Eurodac rules to the forthcoming interoperability framework for the EU information systems and to ensure interoperability with VIS and ETIAS.

As the proposal builds on the existing 2018 agreement between the co-legislators, only targeted amendments to Eurodac rules are proposed. For ease of reference, the text negotiated by co-legislators and compared to the Commission's 2016 proposal is specifically marked and distinguished from the additional amendments proposed. However, neither the full range of Eurodac revisions (the combined 2016 and 2020 revisions), nor the provisions concerning the collection and storage of personal data on persons in admission and resettlement procedures are included in the proposal. This creates a fragmented legal framework and hinders scrutiny of the revisions. It is all the more so considering that there is no Council document detailing the 2018 interinstitutional agreement of the co-legislators, as noted above.

5.1 The Proposed Amendments

Unsurprisingly, the amended proposal does not have too much to add to the overhaul of Eurodac generated by the 2016 proposal, given that the latter already added new categories of persons for whom data should be stored, allowed the use Eurodac to identify irregular migrants, lowered the age for fingerprinting, allowed the collection of identity information together with the biometric data, and extended the data storage period.

Nonetheless, the interaction of Eurodac with other information systems in the framework of interoperability and the greater use of Eurodac in asylum, return and resettlement procedures, mean that the revised Eurodac will serve no fewer than seven purposes:

- a) assistance in the determination of the Member State responsible for examining an application for international protection (the traditional role of Eurodac) and otherwise facilitate the application of the Regulation on Asylum and Migration Management;
- b) assistance in implementing the rules on the EU resettlement framework;
- c) assistance in controlling irregular migration and detecting secondary movements and with the identification of irregular migrants;¹⁶⁰
- d) consultation of biometric data by national law enforcement authorities and Europol;
- e) assistance in the correct identification of third-country national pursuant to Article 20 of the Interoperability Regulations;
- f) support of the ETIAS objectives; and
- g) support of the VIS objectives.¹⁶¹

To serve these ends, the further amendments are proposed, as analysed in the sub-sections below.

5.1.1 Counting Applicants for International Protection in Addition to Counting Applications

With the underlying logic of Eurodac changing to a multi-purpose tool, the proposal marks an important change in the system from counting applications to a database also counting applicants. As indicated in Article 4(6) of the amended Eurodac proposal, where a search is launched with the fingerprints in the

¹⁵⁹ Commission, 'Recommendation of 23 September 2020 on cooperation among Member States concerning operations carried out by vessels owned or operated by private entities for the purpose of search and rescue activities' C(2020) 6468 final; 'Recommendation of 23 September 2020 on legal pathways to protection in the EU: promoting resettlement, humanitarian admission and other complementary pathways' C(2020) 6467 final; 'Guidance on the implementation of EU rules on definition and prevention of the facilitation of unauthorised entry, transit and residence' C(2020) 6470 final.

¹⁶⁰ In that respect, it is welcome that the amended proposal has corrected the incoherent terminology that referred to 'illegal migration'. See ECRE, 'ECRE Comments on the Commission Proposal to recast the Eurodac Regulation' (n 82).

¹⁶¹ Commission, '2020 Eurodac Proposal' (n 7) art 1.

dataset of a third-country national or stateless person and a hit is obtained against at least one other set of fingerprints in another set of data corresponding to that same third country national or stateless person, Eurodac shall automatically link those sets on the basis of the fingerprint comparison, regardless of their category, in one sequence, which would allow the counting of persons. If necessary, the comparison of fingerprints shall be checked and confirmed by a fingerprint expert in accordance with Article 26 of the recast Eurodac Regulation. A notification to eu-LISA that confirms the linking will also be sent.

This change has been deemed necessary due to gaps in information gathering and analysis at EU level. Currently it is not possible to know how many applicants for international protection there are in the EU (and how many of them are applying for the first time), as the Eurodac records refer to applications and several applications referring to the same person may be stored in the system.¹⁶² This reform will also provide the framework for an accurate mapping of onward movements. The amendment should be viewed in conjunction with a revision concerning the role of eu-LISA in producing statistics on the number of asylum applicants and first-time applicants, providing an accurate picture of how many third-country nationals and stateless persons request asylum in the EU.¹⁶³ Statistical data on rejected applications will also be created by the agency. Aggregating these data with other types of information, for example on the number of transfers, will supply the appropriate input for policy responses in relation to unauthorised movements.¹⁶⁴

5.1.2. Cross-System Statistical Data

The compilation of statistical data on the number of applications for international protection is not the sole amendment related to statistics. A new provision, Article 9(3), building on Article 39 of the Interoperability Regulations¹⁶⁵ will enable eu-LISA to draw up cross-system statistics using data from Eurodac, EES, ETIAS and VIS. These statistics are in addition to an elaborate list of statistics that it can produce based on Eurodac data alone, as mentioned earlier. Through these statistics it will be possible to know how many third country nationals were issued a short-stay visa by a specific Member State, followed by legal entry and application for international protection. As indicated in the Explanatory Memorandum, this will “offer the necessary background information for assessing such phenomena and for the appropriate policy response”.¹⁶⁶ Such statistics will be accessed by both the European Border and Coast Guard and the European Asylum Support Office (EASO), within their respective mandates, in the course of producing their analysis on migration and asylum.¹⁶⁷ As indicated in Recital 5c of the amended Eurodac proposal, “[i]n order to specify the content of these cross-system statistics, implementing powers should be conferred on the Commission”.

5.1.3 A New Category for Persons Disembarked Following a Search and Rescue (SAR) Operation and Consistency with the Proposal for a Regulation on Asylum and Migration

Eurodac stores fingerprints of specific categories of applicants for international protection (Category 1), irregular border crossers (Category 2) and irregular migrants (Category 3).¹⁶⁸ The personal scope Eurodac, as expanded by the 2016 proposal and the negotiations, remains the same, albeit with a twist: the amended proposal artificially creates a new category of individuals whose personal data will be stored by distinguishing third-country nationals entering the EU following search and rescue (SAR) operations who apply for international protection from the pool of irregular border crossers.¹⁶⁹ This reform does not alter the treatment of persons disembarked following a SAR operation in terms of the procedure for data collection or the modalities of data storage in Eurodac. The most notable change is that, instead of storing the place of apprehension as envisaged in Article 14(2) of the recast Eurodac Regulation, the revised rules will refer to the place of disembarkation.

¹⁶² Ibid explanatory memorandum, 11.

¹⁶³ Ibid art 9.

¹⁶⁴ Ibid explanatory memorandum, 11.

¹⁶⁵ This provision concerns the creation of a central repository for reporting and statistics (CRRS).

¹⁶⁶ Commission, ‘2020 Eurodac Proposal’ (n 7) explanatory memorandum, 12.

¹⁶⁷ Ibid art 9(3).

¹⁶⁸ Category 4 involves individuals whose fingerprints are consulted for law enforcement purposes.

¹⁶⁹ Commission, ‘2020 Eurodac Proposal’ (n 7) art 14a.

This reform reflects an amendment in the proposal for a Regulation on Asylum and Migration Management as regards the “first country of entry” criterion so as to deem the first country of irregular entry responsible also in the case of persons rescued following SAR operations.¹⁷⁰ Furthermore, the Explanatory Memorandum stresses that this distinction “is indispensable for sustainable and evidence based policy making in the field of migration and visa policy” and will lead to “a more accurate picture of the composition of migratory flows in the EU”.¹⁷¹ Indeed, Article 9 of the amended Eurodac proposal requires the compilation of statistics on the number of persons disembarked following a SAR operation. That said, elsewhere in the proposal, it is noted that border guards cannot apply “the same tools as for irregular crossings by land or air”, such as to define the points of entry.¹⁷² For example, there are no official border checks for SAR arrivals, therefore the points of entry are more difficult to determine and it cannot be specified at which points third country nationals must officially seek entry.¹⁷³

5.1.4 Consistency with the Proposal for a Screening Regulation

One of the legislative initiatives of the New Pact concerns a Proposal for a Screening Regulation introducing a screening process for third-country nationals at the external borders. In a nutshell, the aim of the screening process is twofold: a) to identify the persons concerned, determine whether any individuals pose health and security risks as early as possible; and b) to direct the persons to relevant procedures, be it either asylum or return.¹⁷⁴ To those ends, certain categories of third-country nationals – namely migrants who have entered in unauthorised manner, asylum seekers who entered without authorisation and persons disembarked after a SAR operation –¹⁷⁵ will be subject to pre-screening, which *inter alia* entails identity and security checks through searches in EU and national information systems with the biometric, identity or travel document data or other information provided by the individual concerned.¹⁷⁶ As identification through biometric identifiers is central to the pre-screening process, the amended Eurodac proposal seeks to ensure consistency between Eurodac and the pre-entry screening rules. Consequently, the amended Eurodac proposal foresees that the capturing of biometrics (fingerprints and a facial image) must take place during the screening process. Furthermore, the time limits for taking and transmitting biometric data of applicants to the Central Unit are adapted to mirror the various possible scenarios foreseen in the screening process.¹⁷⁷

5.1.5 New Categories of Personal Data

The proposal requires Member States to insert five new categories of personal data to be collected and stored.

Firstly, when applicable, Member States must indicate that an application for international protection has been rejected, where the applicant has no right to remain and has not been allowed to remain in a Member State, in accordance with the Asylum Procedures Regulation.¹⁷⁸ This reform does not alter either the rights of the rejected applicant, or the applicable rules. It is rather meant to reinforce the link between asylum and return procedures, as well as to provide additional support to national authorities dealing with an applicant for international protection whose application has been rejected in another Member State, as it will allow them to choose the right type of applicable procedure and thus streamline the process.¹⁷⁹ As highlighted, the creation of “a seamless link between asylum and return procedures is [...] more important than ever”.¹⁸⁰

170 Commission, ‘Proposal for Regulation for Asylum and Migration Management’ (n 156) art 13(2).

171 Commission, ‘2020 Eurodac Proposal’ (n 7), explanatory memorandum, 6.

172 Ibid explanatory memorandum, 12.

173 Ibid.

174 Commission, ‘Proposal for a Screening Regulation’ (n 157) art 1.

175 Ibid art 3.

176 Ibid arts 10 and 11.

177 Commission, ‘2020 Eurodac Proposal’ (n 7) art 10.

178 Ibid art 12(x).

179 Ibid explanatory memorandum, 13.

180 Ibid explanatory memorandum, 1.

Secondly, Eurodac will record whether voluntary return and reintegration assistance (AVRR) has been granted to a third-country national, so that Member States can improve their monitoring capacities and prevent “AVRR shopping”.¹⁸¹

Thirdly, information as to whether it appears that the person could pose a threat to internal security will also be indicated.¹⁸² This concerns both the screening process as stipulated in the proposal for a Screening Regulation and the examination pursuant Article 8(4) of the Proposal for a Regulation on the Migration and Asylum Management. This reform was considered necessary in order to enable the implementation of the rules on relocation, as such persons would be excluded from relocation pursuant to the Regulation on Asylum and Migration Management.¹⁸³ In addition, this would speed up the processing of applications for international protection. In that regard, for the applicants for whom a security risk has been flagged and marked in Eurodac, the assessment of the application would focus first on whether this is serious enough to amount to an exclusion/rejection ground for refugees and an exclusion ground for beneficiaries of subsidiary protection.¹⁸⁴ Such a field would be a box that would need to be checked if following verifications during the screening (e.g. in other databases such as SIS, Europol and certain Interpol databases) it becomes apparent the person could represent a security threat.

Fourthly, Eurodac will also note where there are indications that a visa was issued to the applicant, the Member State which issued or extended the visa or on behalf of which the visa has been issued, and the visa application number.¹⁸⁵ The aim of this reform is to facilitate the application of the responsibility criteria for those countries that, though they participate in Eurodac, are not bound by the VIS Regulation and are nonetheless affected by the issuance of a visa. Countries that are specifically assisted by this reform are Ireland, Cyprus, Bulgaria and Romania.

Finally, other rules have been amended to reflect aspects regarding the responsibility of a Member State, namely that Eurodac should indicate the responsible Member State, the shift of responsibility to another Member States, and the cessation of responsibility, as well as the relocation of beneficiaries of international protection.¹⁸⁶

5.1.6 Consequential Amendments

The paragraphs above concern the changes to Eurodac as a standalone database; amendments stemming from the interoperability framework and relating to the access to Eurodac data of other databases could not be made at the time of adoption of the Interoperability Regulations, as Eurodac in its current state does not contain alphanumeric data. In particular, the architectural design of Eurodac will be revised so that identity, travel document and biometric Eurodac data will be stored in CIR, in accordance with the Interoperability Regulations.¹⁸⁷ Furthermore, Article 8a of the amended Eurodac proposal will enable interoperability between Eurodac and ETIAS, so that data in ETIAS applications will be automatically checked against data stored in Eurodac.¹⁸⁸ National visa authorities will also be able to check Eurodac, pursuant to revised VIS rules, so that those authorities may consult records present in Eurodac in a read-only formal prior to making a decision on a visa application.¹⁸⁹ Finally, new access rights are created so that Eurodac data can be consulted by competent visa authorities and the ETIAS National Unit.¹⁹⁰

181 Ibid arts 12(z), 13(2)(q), 14(2)(r) and 14a(2)(q).

182 Ibid arts 12(v), 13(2)(r), 14(2)(s) and 14a(2)(r).

183 Commission, ‘Proposal for Regulation for asylum and migration management’ (n 156) art 57(7).

184 Commission, ‘2020 Eurodac Proposal’ (n 7) explanatory memorandum, 13. See Directive 2011/95/EU of the European Parliament and of the 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 [2011] OJ L 337/9 (Qualification Directive), art 12(2).

185 Commission, ‘2020 Eurodac Proposal’ (n 7) 12(u).

186 Ibid arts 11, 12(l), 14(p); 14b.

187 Ibid recital 6, arts 3 and 4.

188 Ibid art 8a.

189 Ibid art 8c.

190 Ibid arts 8b and 8d.

5.2 Fundamental Rights Assessment

The reforms proposed to Eurodac in the 2020 Pact are arguably of limited extent, as the information system has already undergone major adjustments pursuant to the 2016 proposal and subsequent negotiations between the co-legislators. This does not mean that the fundamental rights implications of the 2020 Eurodac proposal are inconsequential for asylum seekers and irregular migrants. Quite the contrary: in line with the 2016 proposal, Eurodac will progressively eliminate the distinction between asylum seekers and irregular migrants in a security continuum that treats asylum seekers with increased suspicion of (unlawful) onward movement and criminality.

Bringing asylum and migration management under the same legal and policy framework has important legal and practical consequences and may downgrade the protection afforded to asylum seekers and refugees. As such, the proposal follows the growing trend of blurring the distinction between different policy areas: asylum, migration, police cooperation, internal security and criminal justice.¹⁹¹ Eurodac is turning into a multi-purpose information system, with the ultimate aim of exploiting the data collected from persons who may be vulnerable and in need of protection for purposes that may be to their detriment, for example to remove them from the EU territory, or to exclude them from refugee status or from the relocation process. This approach further damages trust between asylum seekers and the state.

Furthermore, Eurodac will cease to operate solely as a support to the Dublin system. It acquires new functions beyond return and irregular migration, to assist in selecting persons for admission procedure, resettlement and relocation, and is elevated to become a primary pool of information for compilation of statistical data to enable informed policy-making.

It is notable that the proposal has not been accompanied by an impact assessment. This makes it the third proposed revision of Eurodac without a prior impact assessment – it is recalled that neither the proposal that led to the enactment of recast Eurodac Regulation nor the proposal of 2016 were accompanied by a fundamental rights assessment. However, the Commission Staff Working Document accompanying the proposal for a Regulation on Asylum and Migration Management does contain an Annex with a limited analysis of the Eurodac revisions.¹⁹²

5.2.1 Interlinking of Eurodac Records: Impact on the Rights to Respect for Private Life and Protection of Personal Data

A substantial change to Eurodac is that all records corresponding to the same third-country national should be automatically linked in a sequence. Up until now, information on onward movements, for example, has relied on assessing proxy indicators, such as Dublin decisions, withdrawn asylum applications, and the number of Eurodac hits involving asylum applicants. These data in the form of proxy indicators concern administrative procedures not persons and entail a certain amount of uncertainty, and thus require checks, such as for false positives (decisions on outgoing take charge Dublin requests for family reasons), double counting or potential omissions of cases, namely cases of expired Dublin responsibility or cases of applications which are made but not lodged.¹⁹³

Whereas these considerations may explain the necessity of the provision, as EDPS highlights, combined with the new categories of personal data that will be collected and further processed in Eurodac and the extensive list of national authorities with access to the data stored, this change is liable to have a substantial impact on the rights to respect for private life and protection of personal data of the concerned individuals.¹⁹⁴ It is thus important to ensure that the retention of Eurodac records is not prolonged beyond the prescribed period for each specific record. For example, if an individual is registered as an irregular border crosser and subsequently applies for international protection, then the record as an irregular border crosser should be automatically deleted after five years. This is in line with pronouncements of the

191 EDPS, 'Opinion 9/2020 - EDPS Opinion on the New Pact on Migration and Asylum (30 November 2020)' 7. As the EDPS notes this trend to blend different objectives has been already evident in the interoperability framework.

192 Commission, 'Staff Working Document Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC)2003/109 and the proposed Regulation (EU)XXX/XXX [Asylum and Migration Fund]' SWD(2020) 207 final.

193 Ibid 101.

194 EDPS, 'Opinion 9/2020' (n 191) 8.

European Courts on the duration of the retention period, as mentioned above.¹⁹⁵ The existence of a link should also be deleted once a record is deleted and should not be visible to national authorities.

Furthermore, in line with the principles of purpose limitation and data minimisation that are incorporated into EU data protection law,¹⁹⁶ additional safeguards must be introduced so that the authorities of Member States and EU bodies continue to be able to see only the data that is relevant for the performance of their specific tasks, even if the records are linked in a sequence.¹⁹⁷

Moreover, information about the possibility of interlinking different data sets of Eurodac should be listed in the information to be communicated to third-country nationals or stateless persons at the time when their biometric data are captured. Finally, the proposal foresees the possibility that the link between two data sets is verified by a fingerprint expert, however, there is no indication as to when such verification will be necessary. Practice shows that, though mandatory in Article 25(4) of the recast Eurodac Regulation, verification of a Eurodac hit by a fingerprint expert does not always take place,¹⁹⁸ therefore it is highly likely that unless clear rules are set out this provision will become dead letter.

Recommendations:

1. The storage period of interlinked records should remain unaltered compared to the recast Eurodac Regulation in effect. Article 4(6) should indicate that the existence of a link should also be deleted once a record is deleted and should not be visible to national authorities.
2. Additional safeguards must be introduced in Article 4(6) that the authorities of Member States and EU bodies should continue to be able to see only the data that is relevant for the performance of their specific tasks, even if the records are linked in a sequence.
3. Information about the possibility of interlinking different data sets of Eurodac should be listed amongst the information to be communicated to third-country nationals or stateless persons at the time when their biometric data are captured (currently under Article 29 of the recast Eurodac Regulation).
4. Clear rules as to when verification of data sets should take place should be indicated in Article 4(6).

5.2.2 Re-Categorisation of Persons Disembarked Following SAR Operations: Which Safeguards for Vulnerable Applicants?

The distinction of persons entering the EU following a SAR operation does not entail any change in their treatment and seems to have been primarily driven by policy considerations and the attempt to produce accurate statistical data. However, the proposal does not take into account that these individuals are highly vulnerable as they have been subject to traumatic experiences during their perilous journeys to reach EU territory, and often before.¹⁹⁹ As a result, the lack of any reference to specific safeguards as regards the procedure for capturing their fingerprint data or the possibility of proscribing the imposition of sanctions in case they do not provide their consent for that capturing must be addressed. It is true that the 2016 Eurodac proposal provides additional safeguards in relation to vulnerable persons subject to Eurodac rules, however the separation of persons disembarked following SAR operations provides an opportunity to specifically link this category with the increased safeguards for vulnerable individuals. The re-categorisation of individuals subject to Eurodac rules should not only facilitate policy-making, but must also work to the benefit of third-country nationals, especially those who may be vulnerable. A recognition in the legislation of their status as susceptible to vulnerabilities is thus crucial.

¹⁹⁵ See Section 4.3.6.

¹⁹⁶ GDPR, arts 5(1)(b) and 5(1)(c).

¹⁹⁷ EDPS, 'Opinion 9/2020' (n 191) 8.

¹⁹⁸ For example, see Administrative Court of Appeal of Lyon, 20 November 2018, N° 18LY01453, available at: <https://bit.ly/3bVsVSw>, accessed 31 December 2020.

¹⁹⁹ See to that effect Moritz Baumgärtel, 'Facing the Challenge of Migratory Vulnerability in the European Court of Human Rights' (2020) 38(1) Netherlands Quarterly of Human Rights 12. Baumgärtel more generally refers to migratory vulnerabilities of varying extent, linked to the fact that a person once crossed or tried to cross national borders.

Recommendation:

In relation to individuals disembarked following SAR operations increased safeguards should be included, particularly by explicitly referring that the safeguards concerning vulnerable individuals are applicable to them. This reference could be added to both Article 2 (on the obligation to capture biometric data) and Article 14a, which concerns the collection and transmission of biometric data of persons disembarked following SAR operations.

5.2.3. Overemphasis on the Production of Statistical Data

The reconfiguration of the categories of third-country nationals and stateless persons falling under Eurodac illustrates an overemphasis on developing statistical data from Eurodac records on its own or in combination with records pulled from other information systems.

In that respect, three considerations must be kept in mind:

- First, there should not be overreliance on the accuracy of information stored in Eurodac (and other operational information systems for that matter). As numerous reports have indicated, the quality of information systems may suffer in various respects (spelling errors, lack of documentation, insufficient language skills, etc).²⁰⁰ Whereas the production of statistical data will rely on anonymised information – therefore all that matters is the correct categorisation of individuals registered in the system – the possibility that national authorities arbitrarily categorise third-country nationals under Category 1 or Category 2 cannot be overruled.²⁰¹
- Second, the production of statistical information does not feature amongst the objectives of Eurodac, even though it is clear that several of the reforms have been triggered by the need for informed policy-making. Instead, it is submitted that statistical information is considered as ultimately serving the objective of tackling irregular migration and secondary movements.²⁰² This is a both vague and indirect objective. For example, Article 6(1)(h) of the EES Regulation provides that one of the purposes of that information system is to gather statistics on the entries and exits, refusals of entry, and overstays of third-country nationals in order to improve the assessment of the risk of overstays and support evidence-based EU migration policy making.
- Third, it is not clear why the cross-system statistics are not explicitly defined in the amended Eurodac proposal and their determination of the scope and content will take place by the Commission through implementing acts. The explanatory memorandum provides as an example the development of statistics concerning third-country nationals who have been granted Schengen visas and have subsequently applied for international protection. However, this is not reassuring. In fact, it is rather worrying how this information will be used for policy-making and what the fundamental rights implications of such information will be for asylum seekers who may be significantly hindered in accessing the EU territory.

As a result, the combined use of information stored in databases may be used to prevent asylum seekers from reaching the EU territory, which is the precondition for applying for international protection, and thus the exercise of the right to seek asylum, as outlined in Article 18 of the Charter may be hindered. Information on individuals seeking legal ways to access EU territory to lodge their application for international protection may be weaponised to prevent access and this may in turn drive individuals to use irregular routes. For example, statistical data may demonstrate a trend whereby nationals of a

200 Fundamental Rights Agency, Opinion 1/2018 30; European Court of Auditors, 'EU information systems supporting border control – A strong tool but more focus is needed on timely and complete data' (2019).

201 In that respect see 'EU's migrant fingerprinting system Eurodac under review' (DW, 9 November 2017), available at: <https://bit.ly/39NvbbW>, accessed 31 December 2020. This is not a hypothetical issue. In 2016, a Dublin transfer on the basis of a Eurodac match was disputed before the Administrative Tribunal of Nantes. The case involved a Cameroonian who, after having been subject to an expulsion order from Spain for having entered irregularly, applied for international protection in France. Though his transfer to Spain was ordered based on the Eurodac hit, other documents in the file, including an interview carried out by the Spanish authorities, showed that he had in fact been apprehended as an irregular border-crosser and had not filed an asylum claim in Spain. Therefore, the transfer decision was based on erroneous information and was thus quashed, also because the applicant's personal circumstances were not examined. See Tribunal Administratif de Nantes, Jugement du 18 février 2016, No. 1600829, available at: <https://bit.ly/3p844OY>, accessed 31 December 2020.

202 Commission, 'Staff Working Document' (n 192) 101.

particular third country obtain a Schengen visa and subsequently when they reach the EU territory they apply for international protection. Such correlations could be made known to consulates so that individuals from that third country are not (easily) granted a Schengen visa.

Recommendations:

1. The production of statistical data, as envisaged in Article 9, should be coupled by rules requiring the rectification of incorrect data within specific deadlines. Otherwise, the statistical data may provide incorrect information. This addition could take place by amending Article 28 of the recast Eurodac Regulation on the right to access, rectification and deletion of personal data.
2. The scope of cross-system statistics, as laid down in Article 9(3), should be clarified so that it is avoided that data in connection to individuals who pursue legitimate activities are weaponised to deny access to EU territory to individuals in need of international protection

5.2.4. Adding a Security Flag: Long Lasting Impact on the Individual

Another aspect that merits further exploration concerns the insertion of a security flag following a security check during the screening process, in accordance with Article 11 of the proposal for a Screening Regulation or Article 8(4) of the proposal for a Regulation on Asylum and Migration Management.

This security check will entail queries with relevant national and EU databases, as well as gathering information on refusals of a travel authorisation, refusals of entry, or decisions to refuse, annul or revoke a visa or residence permit when based on security grounds.²⁰³ The addition of this category of personal data to be stored does not entail collecting personal data *per se*, however, it does entail the storage and the processing of personal information, thus the rights to respect for private life and protection of personal data are affected. Importantly, it constitutes an assessment of the individual in question, which by default constitutes information that is not verifiable via documentation and is based on a rapid assessment of the individual. As a result, the quality of this type of personal data stored may be particularly suspect.

The fundamental rights implications of the screening process have been analysed by ECRE in comments on the Screening Regulation.²⁰⁴ It suffices here to point out that deciding whether an individual may constitute a security risk must be based on accurate, reliable data, particularly in view of the important consequences that such flagging may have for an application of an asylum seeker or for their prospects of relocation to another Member State.

Overall, any irregularities, arbitrariness or strictness in the security assessment of individuals is bound to have a long-lasting impact on those persons via the storage of the security flag. This is all the more important considering that practice shows that the rights to access, rectification and deletion of Eurodac records are rarely exercised.²⁰⁵ The right to information should be further extended so that individuals are informed about their potential flagging in Eurodac as security risks.

Recommendations:

1. The storage of a security flag must be accompanied by increased safeguards as this information is not always verifiable and is based on a speedy assessment of the individual concerned, which may however have long lasting, negative consequences for the persons concerned.
2. Individuals should be informed about the storage of the security flag, in accordance with the right of information (currently envisaged in Article 29 of the recast Eurodac Regulation).

203 Commission, 'Proposal for a Screening Regulation' (n 157) arts 11(2) – 11(3).

204 ECRE, Comments on the commission proposal for a screening regulation com(2020) 612, November 2020, available at : <https://bit.ly/3iy2h3i>.

205 The great majority of Member States have not recorded any requests for access since July 2016. See; Eurodac Supervision Coordination Group, 'Report on the Exercise of Data Subjects' Rights in Relation to Eurodac (2019) 9, available at: <https://bit.ly/2LUKHUm> , accessed 31 December 2020; FRA, 'Under Watchful Eyes – Biometrics, EU IT-Systems and Fundamental Rights' (27 March 2018), available at: <https://bit.ly/3p4eYoR> , accessed 31 December 2020 100-101. For an analysis see Vavoula, 'Between Gaps in Judicial Protection and Interstate Trust' (n 8).

5.2.5 Supervision

The independent supervision of the data processing activities under the recast Eurodac Regulation, both at EU and national level, is a key guarantee for the effective protection of the

fundamental rights to respect for private life and protection of personal data, in line with Article 8(3) of the Charter. Cooperation between national data protection authorities and the EDPS is ensured by Article 62 of the GDPR, which sets out a single model of coordinated supervision of information systems within the framework of the European Data Protection Board (EDPB). Since 2019, the EDPB has established a dedicated Coordinated Supervision Committee. As the EDPS has pointed out, the proposal should make reference to this new model of coordinated supervision.²⁰⁶

Recommendation:

Reference to the revised model of coordinated supervision of Eurodac must be made by revising the rules on coordinated supervision between national supervisory authorities and the EDPS, as currently envisaged in Article 32 of the recast Eurodac Regulation.

5.2.6 Consequential Amendments

Finally, the amended proposal also details how Eurodac will interact with other systems in an interoperable framework, namely ETIAS and VIS, by enabling automated processing of Eurodac records in order to enable informed decision-making on visa and ETIAS applications. The Interoperability and ETIAS Regulation have already been adopted and in December 2020 the co-legislators agreed on a revised VIS legal framework. Therefore, though the implications of interconnecting Eurodac with ETIAS and VIS so as to enable automated processing of Schengen visa and ETIAS applications cannot be discarded, the reforms in Eurodac in connection to enabling interoperability are pre-determined in order to align the Eurodac rules to the prescriptions of other information systems. However, the wording used in the stated purposes that Eurodac will support the VIS and ETIAS objectives is somewhat problematic, because this wording seems to denote that Eurodac absorbs the objectives of those information systems. That said, this wording was preferred in the legal instruments of other databases and therefore it is unlikely to change.²⁰⁷

6. CONCLUDING REMARKS - RECOMMENDATIONS

The analysis above demonstrates that Eurodac is progressively being transformed from an information system of limited aims and capacities into a support tool for a range of EU policies on asylum, resettlement and irregular migration. The amended proposal in the framework of the New Pact on Migration and Asylum builds on the 2016 proposal as negotiated by the co-legislators and further dismantles the distinctions between policies of irregular migration and asylum by progressively merging the treatment of asylum seekers and irregular migrants. The proposal presents certain challenges to the protection of fundamental rights, particularly with regard to the rights to respect for private life, protection of personal data, the rights of the child and the right to asylum.

In line with the findings of the previous Sections in relation to the 2020 amended Eurodac proposal, this paper puts forward the following recommendations:

- The **storage period of interlinked records should remain unaltered**. Article 4(6) of the revised Eurodac Regulation should indicate that the existence of a link should also be deleted once a record is deleted and should not be visible to national authorities.
- **Additional safeguards** must be introduced in Article 4(6) that the authorities of Member States and EU bodies should continue to be able to see only the data that is relevant for the performance of their specific tasks, even if the records are linked in a sequence.

²⁰⁶ EDPS, 'Opinion 9/2020' (n 191) 8-9.

²⁰⁷ For example see ETIAS Regulation, art 4.

- **Information about the possibility of interlinking** different data sets of Eurodac should be listed amongst the information **to be communicated** to third-country nationals or stateless persons at the time when their biometric data are captured (currently under Article 29 of the recast Eurodac Regulation).
- **Clear rules as to when verification of data sets should take place** should be indicated in Article 4(6).
- In relation to individuals **disembarked following SAR** operations **increased safeguards** should be included, particularly by explicitly referring that the safeguards **concerning vulnerable individuals** are applicable to them. This reference could be added to both Article 2 (on the obligation to capture biometric data) and Article 14a, which concerns the collection and transmission of biometric data of persons disembarked following SAR operations.
- The **production of statistical data**, as envisaged in Article 9, should be coupled by rules requiring the **rectification of incorrect data within specific deadlines**. Otherwise, the statistical data may provide incorrect information. This addition could take place by amending Article 28 of the recast Eurodac Regulation on the right to access, rectification and deletion of personal data.
- The **scope of cross-system statistics**, as laid down in Article 9(3), **should be clarified** so that it is avoided that data in connection to individuals who pursue legitimate activities are weaponised to deny access to EU territory to individuals in need of international protection.
- **The storage of a security flag must be accompanied by increased safeguards**, as this information is not always verifiable and is based on a speedy assessment of the individual concerned, which may however have long lasting, negative consequences for the persons concerned.
- **Individuals should be informed about the storage of the security flag**, in accordance with the right of information (currently envisaged in Article 29 of the recast Eurodac Regulation).
- Reference to the revised model of coordinated supervision of Eurodac must be made by **revising the rules on coordinated supervision between national supervisory authorities and the EDPS**, as currently envisaged in Article 32 of the recast Eurodac Regulation.



ecre

European Council
on Refugees and Exiles

European Council on Refugees and Exiles

Avenue des Arts 7/8

Brussels 1210

Belgium

T.+32 232 900 40

ecre@ecre.org

www.ecre.org