Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status

statewatch

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON UNDOCUMENTED MIGRANTS

PICUM

PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

statewatch

This report was written by Chris Jones, Researcher at Statewatch, as a background document for a legal seminar organised on 14-15 November 2019 in Brussels by PICUM, the Centre for European Policy Studies (CEPS) and European Migration Law.

PICUM gratefully acknowledges the support of Emer Connor, PICUM trainee, for her assistance in finalising the report.

The legal seminar and the preparation of this report were made possible through the generous support of:

European Commission

SIGRID RAUSING TRUST

OPEN SOCIETY FOUNDATIONS

ADESSIUM FOUNDATION

OAK FOUNDATION

Epim European Programme for Integration and Migration

This report has received financial support from the European Union Programme for Employment and Social Innovation "EaSI" (2014-2020). For further information please consult: http://ec.europa.eu/social/easi. The information contained in this publication does not necessarily reflect the official position of the European Commission

Contents

Executive Summary

This paper examines the EU's justice and home affairs databases and information systems, the changes that have been introduced by recent legislation seeking to make those systems 'interoperable' and the potential implications of those changes for fundamental rights, in particular in relation to undocumented migrants. Notwithstanding concerns over the necessity and proportionality of the interoperability initiative as a whole, the new rules lack the necessary safeguards to protect people from the arbitrary, unjustified or excessive exercise of state power. With key details left to national government decisions, closely monitoring the implementation of these rules will be crucial to uphold the rights of undocumented migrants and other parts of the population.

Massive data processing to facilitate increased identity checks

One key aim of the interoperability initiative is to facilitate an increase in police identity checks of non-EU nationals, whether documented or undocumented. To this end, a huge new database – the **Common Identity Repository (CIR)** (see Fig. 1), with a capacity of up to 300 million records containing biographic and biometric data – is being constructed, making use of data in a number of existing and forthcoming EU databases.

This paper focuses on four main issues arising from the legislation governing how national authorities should use the CIR for carrying out identity checks:

- while the legislation contains anti-discrimination safeguards, they are extremely weak;
- there is no evidence to suggest that non-EU nationals are more likely than EU nationals to be engaged in activities threatening public security or public policy, calling into question the proportionality of allowing access to the CIR for the broad purpose of "ensuring a high level of security", as it suggests that non-EU nationals *a priori* constitute a security threat;
- the legislation does not precisely circumscribe the specific offences or legal thresholds that could justify access to the database; and
- depending on the way Member States implement EU rules on data protection in the criminal justice and law enforcement sector, the CIR could be used to undermine 'firewalls' between public services and immigration enforcement.

Repurposing data from underlying IT systems

The way the CIR is being constructed also runs counter to a key data protection principle. The data it will contain (at least one biometric identifier and basic biographic details, in essence equivalent to that available in the chip of a biometric passport) is to be extracted from a number of existing and forthcoming systems (**EES**, **ETIAS**, **Eurodac**, **SIS**, **VIS** and **ECRIS-TCN**, see Figure 2). As well as being used to facilitate identity checks and assist in criminal investigations via the CIR, this data will be subject to large-scale, automated cross-checking to try to detect the use of multiple identities by non-EU nationals, through the introduction of a system called the Multiple Identity Detector (MID).

These underlying databases were set up for specific purposes, such as the issuance of short-stay Schengen visas (the VIS) or the registration of crossings of the external Schengen borders (the EES). The use of data for new purposes that were

never foreseen in the original legislation – as will be done with the CIR and the MID – undermines the principle of purpose limitation: personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".[1] While the relevant legislation has been amended to graft new purposes onto the existing systems, the necessity and proportionality of doing so is highly questionable.

Existing systems reformed for an expanded role in detection and expulsion

Recent and ongoing changes to the legislation governing the EU's databases do not only seek to ensure that the information they hold can be used in the CIR and the MID. Three long-standing databases – the **Schengen Information System**, **Eurodac** and the **Visa Information System** – have recently been or are being reformed. A key aim of the changes is to expand their role in the detection and expulsion of those with no right to remain in the Schengen area.

The changes to Eurodac (for which negotiations are ongoing) will have a particular impact on undocumented migrants. The Eurodac proposal seeks to transform what is currently an asylum database into one for "wider immigration purposes" by introducing the five-year storage of personal data from third-country nationals or stateless persons found irregularly staying in a Member State. The aim is to help identify those who should be subject to expulsion orders and provide "precious elements of evidence for re-documentation and readmission purposes."[2]

Currently, data on this category of persons may be checked against the central Eurodac database (which holds the fingerprints of asylum-seekers and individuals apprehended in connection with irregular border-crossings) but it is not stored. If the changes are approved as proposed, their data would be stored in Eurodac and also added to the CIR, where it would be used to facilitate identity checks aimed at detecting undocumented migrants. Even without these changes, however, the absence of an individual from the CIR may lead to suspicion on the part of the authorities regarding their immigration status.

A fundamental shift in data processing to support immigration and law enforcement

The interoperability initiative will introduce fundamental changes to the structure and operation of the EU's justice and home affairs databases and the processing and use of the personal data they contain. In relation to the 'identity data' of non-EU nationals, the interoperability rules introduce a "single, overarching EU information system" – something that just a decade ago the European Commission argued would "constitute a gross and

1 Article 5(1)(b), General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

2 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac', COM(2016) 272 final, 4 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272

Figure 1: New interoperability systems expected to be in place by 2023

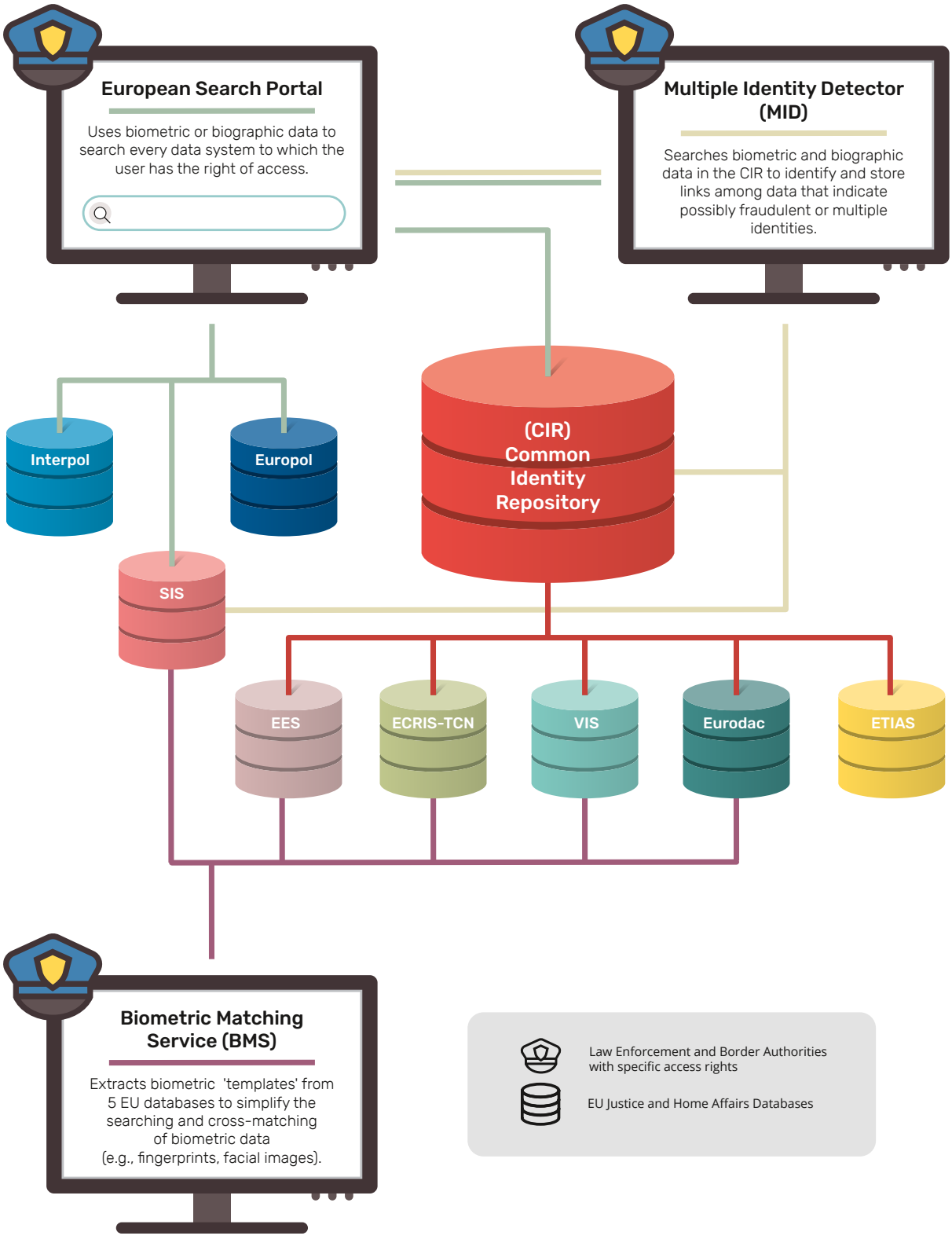
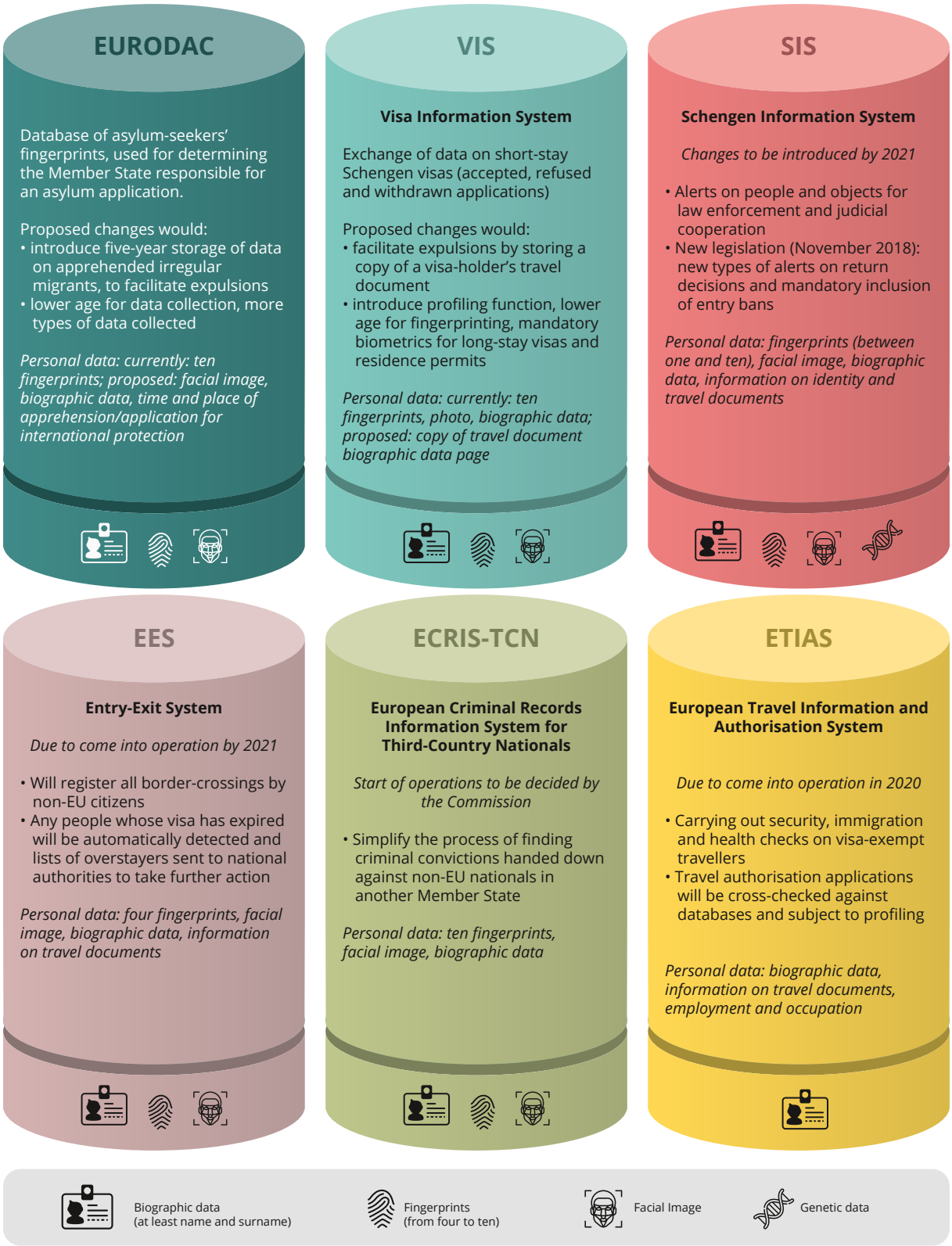


Figure 2: **Existing and forthcoming EU Justice and Home Affairs databases**



illegitimate restriction of individuals' right to privacy and data protection."[3]

At the same time, the databases underlying the new 'interoperable' systems are being altered to try to more effectively and efficiently locate and expel those who are irregularly present in the Schengen area, through the processing of more personal data, gathered from a greater number of people, for a broader set of purposes. The potential effects for non-EU nationals, including undocumented migrants, are likely to be significant. Migrants' rights and privacy advocates should pay close attention to the changes being introduced at EU level, the framing of forthcoming national legislation concerning identity checks, the development and implementation of the systems themselves and emerging plans that seek to expand the new 'interoperable' systems to include EU nationals.

3 European Commission, 'Overview of information management in the area of freedom, security and justice', COM(2010) 385 final, 20 July 2010, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/intro/docs/com_2010_385_en.pdf

1. Migration control and border management: existing EU systems

1.1. Overview

The introduction of large-scale information systems and databases has been instrumental to the implementation of EU law and policy in the field of justice and home affairs. Three systems are currently in use, serving a variety of purposes:

- sharing police, judicial and other data in order to compensate for the Schengen area of free movement (the **Schengen Information System, SIS**, in operation since 2001);
- assisting in determination of the state responsible for processing an asylum application (**Eurodac**, established in 2000); and
- making information available across the Schengen area on short-stay visa applications (the **Visa Information System, VIS**, in full operation since 2015).

These three long-standing systems have recently been or are being reformed, expanding their purposes and the amount of data they process. They will also soon be complemented by three further systems:

- an **Entry/Exit System (EES)** to monitor border crossings and detect people whose visa has expired, due to come into operation in 2021;
- a E**uropean Travel Information and Authorisation System (ETIAS)** to carry out security, immigration and health checks on visa-exempt travellers, due to come into operation in 2020; and
- a **European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)** to simplify the process of finding criminal convictions handed down against non-EU nationals in another Member State, with the start of operations to be determined by the European Commission.[4]

For more detailed information about these information systems, see Annex 6. The data they hold overwhelmingly concerns non-EU citizens ('third-country nationals')[5] and they play a key role in attempts to locate, expel and exclude those with no right to be in the Schengen area, including both those who entered with permission and those who did not. The following sections examine: firstly, the use of these systems for identifying those who entered with the correct papers but have stayed longer than permitted and those who have entered and stayed without permission; and secondly, the use of these systems for the purposes of expelling and excluding people from the EU.

4 Article 35, Regulation (EU) 2019/816, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0816

5 Eurodac, the VIS, the EES and the ETIAS only process data on non-EU citizens. ECRIS-TCN will mainly process data on non-EU citizens, but some EU citizens who have dual nationality with a non-EU state will also be included in the system. The SIS can process data on both EU citizens and non-EU citizens.

1.2. Detecting people whose visa has expired and those who entered irregularly

Although there is little hard evidence on the topic, it is widely assumed that a significant proportion of undocumented persons in the EU are in possession of expired visas. The VIS (which is already in operation but is the subject of ongoing legislative negotiations) and the forthcoming EES have a key role in dealing with this category of person.

The storage of biometrics in the VIS (ten fingerprints and a facial image) allows border guards and other officials to check whether the person in possession of a visa is its rightful owner. The system is also used to prevent an individual making multiple visa applications in different Schengen states (rejected and withdrawn applications are also stored in the system). Changes proposed by the European Commission in May 2018, which are currently under negotiation, will expand the system's scope to include data on long-stay visas and residence permits, as well as lowering the age for the inclusion of biometrics in the system (from 14 to six years).[6]

The VIS is unable to automatically calculate the length of time a short-stay visa-holder may remain in the Schengen area, a task which must be carried out by examining the entry and exit stamp(s) placed in an individual's passport. The introduction of the EES is intended to resolve this problem. The system will cover both non-EU nationals who require visas and those who do not, replacing the ink-on-paper charm of passport stamps with a centralised database that will be used to register the time, date and location of an individual's border crossings. When an exit is not recorded in an individual file within the required time limit, details will be transmitted from the central system to the relevant national authorities, so that they can "adopt appropriate measures,"[7] in accordance with national law, for removing the individual.

Of course, knowing who has overstayed will not automatically make it possible to locate them, and it seems likely that making full use of the information provided by the EES would require significant investment in the enforcement personnel and infrastructure needed to detect and expel people. Nevertheless, as the Commission has explained, the combined data held in the EES and VIS will allow national authorities to "identify any undocumented irregular migrant found within the territory that crossed the external border legally; this will in turn facilitate the return process."[8]

Another group of persons who have been the subject of significant attention from politicians and policy-makers in recent years are those who cross the external Schengen borders irregularly and remain without authorisation. Changes to Eurodac are intended to address an 'information gap' concerning this group.

Currently, Eurodac stores the fingerprints of asylum seekers (known as 'Category 1') and

6 Other novelties introduced by the proposal include the mandatory inclusion of biometrics in long-stay visas (an issue currently left to national rules) and a system for profiling visa applicants. See: 'All visa applicants to be profiled and children fingerprinted for revamped Visa Information System', *Statewatch News*, 17 August 2018, http://www.statewatch.org/news/2018/aug/vis-profiling-child-fingerprinting.htm; 'Visa Information System: Commission proposals sneak in mandatory biometrics for long-stay visas', *Statewatch News*, 20 August 2018, http://www.statewatch.org/news/2018/aug/vis-fingerprints-long-stay-visas.htm; 'Visa Information System: child fingerprinting and police access proposals criticised by data protection authorities', *Statewatch News*, 21 August 2019, http://www.statewatch.org/news/2019/jan/eu-vis-scg-letter.htm

7 Article 12(3), Regulation (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

8 Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES), COM(2016) 194 final, 6 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0194

individuals apprehended in connection with irregular border-crossings ('Category 2'), with the aim of facilitating the 'Dublin' rules on determining the member state responsible for processing applications for international protection. Capturing and comparing fingerprints makes it possible for national authorities to determine whether another Member State should be responsible for handling an individual's application.

Fingerprints can also be taken from third-country nationals or stateless persons found irregularly staying in a Member State ('Category 3').[9] These are not currently stored in the central database but are compared to the other datasets to establish whether an individual has previously applied for asylum or irregularly crossed an external border. The 2016 proposals would change this by storing fingerprint and other data on this category of person for five years.[10] As the proposal explains:

> *"Extending the scope of EURODAC will allow the competent immigration authorities of a Member State to transmit and compare data on those illegally staying third-country nationals who do not claim asylum and who may move around the European Union undetected. The information obtained in a hit result may then assist competent Member State authorities in their task of identifying illegally staying third-country nationals on their territory for return purposes. It may also provide precious elements of evidence for re-documentation and readmission purposes."*[11]

As with the VIS, the proposal aims to lower the age limit for data collection in Eurodac (for all three categories of person) from 14 to six years. New categories of data are also to be stored in the system, including facial images. This, the Commission noted in the proposal, "will prime the system for searches to be made with facial recognition software in the future."[12]

9 Chapter IV, Regulation (EU) 603/2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603

10 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac', COM(2016) 272 final, 4 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272

11 Ibid.

12 Ibid.

1.3. Stepping up expulsion and exclusion

Assuming that the revamped and new systems being introduced are successful in their goals of detecting greater numbers of people whose visa has expired and irregular migrants, the presumption is that they will subsequently be expelled from the Schengen area. Here too, the EU's databases and information systems are supposed to come to play an increasing role.

As already noted, the inclusion in Eurodac of more personal data on a new category of persons means the system could provide evidence for "re-documentation and readmission" to the country of nationality or a non-EU 'transit' country. The expansion of VIS is also supposed to assist with this – alongside the changes being made outlined above, the proposed new rules would require the inclusion in the central database of a copy of every short-stay visa applicant's travel document.

Currently, a copy of the travel document is stored by the consulate or embassy at which an individual makes their application. If the authorities wish to remove that person from the EU, they must make contact with the relevant consulate or embassy, a potentially time-consuming process. Under the proposal's new rules, "migration and return authorities… would be able to retrieve this [centrally-stored] copy, subject to strict access rules." The intention is clear: "to help identify and return irregular migrants."[13]

The SIS is now governed by three Regulations approved in 2018, of which one key aim is to beef up the system's role in enforcing return orders and entry bans handed down against non-EU nationals.[14] It will now become mandatory for all Member States to insert information on return decisions and their enforcement into the SIS,[15] something that was previously dependent on national law.[16] The proposal for the new rules argued that individuals could "avoid or prevent the enforcement of an existing [return] decision by simply moving to another Member State," where the authorities might apprehend the person in question, but be unaware of the decision previously issued elsewhere. In such cases "the apprehending Member State would therefore need to re-launch return procedures from scratch, further prolonging the illegal stay and delaying the return of the irregular migrant."[17] The mandatory sharing of information on return decisions is intended to overcome this problem.[18]

The expanded use of entry bans, for excluding people from the Schengen area for potentially years at a time, has also been introduced by changes to the SIS legislation. Further changes are

13 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, COM(2018) 302 final, 16 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

14 There are three new Regulations (see Annex 1). Two are relevant for the purposes of this discussion: Regulation (EU) 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1860; and Regulation (EU) 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1861

15 Article 3, Regulation (EU) 2018/1860

16 Combined with 2017 rules on border checks, this should lead to an increase in the number of departures registered through the system. Mandatory systematic checks of all individuals entering and exiting the EU were introduced by changes to the Schengen Borders Code that came into force in April 2017, meaning that the voluntary departure of any individual subject to a return decision will be registered. Those subject to forced return proceedings will also have their departure recorded in the SIS. Article 6 of Regulation 2018/1860 sets out the procedure for registering departures of individuals subject to return decisions.

17 Proposal for a Regulation on the use of the Schengen Information System for the return of illegally staying third-country nationals, COM(2016) 881 final, 21 December 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0881

18 It should be borne in mind that unawareness of other Member States' decisions is not the only reason for a lack of mutual recognition and enforcement. In a majority of Member States national legislation provides the possibility to recognise return decisions issued by another Member State under certain conditions, but they do not necessarily do so. A 2017 study by the European Migration Network found that "in practice, several of these Member States indicated that they never or rarely enforced such a return decision. The main challenge invoked for mutual recognition is the difficulty in knowing whether a return decision has effectively been issued by another Member State and whether it is enforceable." See: European Migration Network, 'The effectiveness of return in EU Member States', 15 February 2018, p3, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_return_study_en.pdf

also under discussion in the context of amendments to the Returns Directive.

SIS alerts on refusal of entry to or stay in the Schengen area have consistently been the largest category of alerts on persons stored in the system and under the new rules their number is likely to increase.[19] The previous legislation only allowed these alerts to be issued if a non-EU national was convicted of an offence "carrying a penalty involving deprivation of liberty of at least one year," when there were "serious grounds for believing that he [had] committed a serious criminal offence" or had clear intentions to do so, or when a person was "subject to a measure involving expulsion, refusal of entry or removal… that includes or is accompanied by a prohibition on entry or, where applicable, a prohibition on residence."[20] These provisions are maintained in the new Regulation[21] and are accompanied by a new requirement to enter an alert on refusal of entry or stay whenever an entry ban is issued in accordance with the Returns Directive.[22]

To cast the net even wider, the relevant provisions in the Return Directive may also be altered. Currently, return decisions handed down in accordance with the Directive must be accompanied by an entry ban "if no period for voluntary departure has been granted" or "the obligation to return has not been complied with."[23] However, a proposal published in September 2018 would introduce more obligatory grounds for denying a period of voluntary departure,[24] as well as a new possibility for national authorities to hand down entry bans to non-EU nationals who have been irregularly present on the territory of the Member States and whose irregular stay "is detected in connection with border checks carried out at exit."[25] Negotiations on the recast Returns Directive proposal are ongoing.

The European Border and Coast Guard Agency, Frontex, also has a key role in the drive to increase expulsions. Under the new SIS rules, the agency will have access to the database for a number of reasons. For example, it will be possible for members of Frontex return teams to use the SIS to examine the expulsion orders issued to people facing deportation on a Frontex-coordinated flight, to ensure that those orders remain in force – a useful safeguard, if the national authorities ensure that the relevant information is up-to-date.[26]

Perhaps more significant, however, is the development by Frontex of its own data processing systems for the purpose of coordinating expulsion

19 Between 2009 and 2018, an average of 598,941 alerts on individuals to be refused entry or stay were stored in the SIS at each year's end. See the chart in Annex 2 for further details.

20 Article 24(2), Regulation (EC) No 1987/2006, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32006R1987

21 Article 24(1)(a), Regulation (EU) 2018/1861

22 Article 24(1)(b), Regulation (EU) 2018/1861

23 Article 11(1), Directive 2008/115/EC

24 Currently, "Member States may refrain from granting a period for voluntary departure, or may grant a shorter period than seven days" if there is a risk of the individual absconding, if an application for legal stay is deemed fraudulent or manifestly unfounded, or if they are considered a "risk to public policy, public security or national security." Under the Commission's proposal, in such cases "Member States shall not grant a period for voluntary departure."

25 Article 13(2), 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 2018/0329 (COD)

26 In 2015 the Council of Europe's Committee for the Prevention of Torture monitored a Frontex-coordinated deportation from Italy. They interviewed 13 Nigerian women due to be removed and found that they had all appealed against the initial rejection of their asylum applications. Although this did not automatically suspend the removal orders, the expulsion of seven of those women was subsequently halted before the flight departed. In the case of one woman, "the competent court had decided to grant suspension of removal," but this was only communicated to the authorities "after the joint flight had departed from Rome airport." The report highlighted that: "No information as to the pending legal procedures could be found in the women's removal files. Apparently, such a state of affairs is not unusual." In such a case, checks by Frontex officials in EU databases may well reveal nothing regarding ongoing legal proceedings that could provide grounds to halt deportation proceedings and, in the words of the CPT, prevent "a potentially irreversible effect in breach of Article 3 of the European Convention on Human Rights". See: Report to the Italian Government on the visit to Italy carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 16 to 18 December 2015, http://hudoc.cpt.coe.int/eng?i=p-ita-20151216-en-2

operations. Through the Frontex Application for Return (FAR), the agency receives from national authorities the personal data of individuals due to be expelled from the EU. The current data protection rules for FAR include the possibility to prevent individuals from accessing their data – the right of access may be "restricted on a case-by-case basis… for reasons of national security, public security and defence of the Member States."[27] This restriction, if used, would make it impossible to exercise the rights to correction, deletion or alteration, increasing the possibility of erroneous deportations.[28] The 2019 Frontex Regulation maintains the possibility of such exemptions and requires that the agency adopt specific internal rules on the issue in the context of removal operations.[29] (It should be noted that FAR is currently not in any way related to the interoperability initiative.)

Taken together, the EU's databases and information systems are coming to play an increasingly significant role in the control and management of migration, covering the time prior to an individual's entry to the Schengen area, the moment at which they cross the border, their time within the Schengen area, their departure (whether voluntary or forced) and beyond. While the legal basis for this information architecture is almost complete (for the time being), negotiations are still ongoing on the new Eurodac and VIS proposals, providing an opportunity to challenge their more contentious elements.

Despite the increasing connections between the aims of these databases, their gradual development and compartmentalised structure reflects the different purposes for which they have been introduced. This has been recognised as a useful privacy protection – keeping personal data in separate systems helps to minimise access and also lowers the risks posed by any data breach. However, there has long been political pressure to more systematically combine, share and compare the data held in these different systems – in particular with regard to the two distinct policy objectives of combating terrorism and managing migration – and in recent years that pressure has finally developed into action.

27 It is not clear from the data protection notice whether it is Frontex or the Member States that determine whether or not to apply the restrictions. It is presumably the latter, as Frontex has no competences concerning national security, public security or defence. See: 'Data protection notice for Frontex Application for Return (FAR)', undated, https://frontex.europa.eu/assets/Data_Protection/Data_Protection_Notice_Returns.pdf

28 A comparison can be drawn with the 'immigration exemption' in the UK Data Protection Act 2018, which 'allows the government and others to ignore the EU's data protection rules when those rules get in the way of "the maintenance of effective immigration control' or 'the investigation or detection of activities that would undermine the maintenance of immigration control.'" See: 'Press release – Advocates bring first GDPR complaint to EU against UK data protection law for violating data rights of foreigners', PICUM, 1 July 2019, https://picum.org/press-release-advocates-bring-first-gdpr-complaint-to-eu-against-uk-data-protection-law-for-violating-data-rights-of-foreigners/

29 Article 87(2), Regulation of the European Parliament and of the Council on the European Border and Coast Guard (text as agreed between the Council and Parliament), http://www.statewatch.org/news/2019/apr/eu-frontex-final-tAnnex%20to%20LIBE%20letter-EBCG-text.pdf

2. The interoperability initiative

2.1. Background

In 2017, the European Commission convened a 'high-level expert group on information systems and interoperability' (HLEG) to "identify and address shortcomings and information gaps caused by the complexity and fragmentation of information systems at European level," and to elaborate the "legal, technical and operational aspects of options to achieve interoperability of information systems, including their data protection implications." Regarding interoperability, the group's May 2017 recommendations called for the establishment of:

- a **European Search Portal** (to search across all relevant systems simultaneously);
- a shared **Biometric Matching Service** (to process biometric data from all existing and new systems, reducing costs and complexity); and
- a **Common Identity Repository** (to "allow a complete view of all claimed biographic identities used by a person").

Legal proposals from the European Commission followed in December 2017, adding a further element – a **Multiple Identity Detector** that would search across biometric and biographic data from all existing systems simultaneously. Agreement between the Council and Parliament was rapidly reached – just in time for the European Parliament elections in May 2019 – and the proposals became law in June 2019.[30]

This legislation is unlikely to be the last on the issue of interoperability in the field of justice and home affairs. The new measures primarily concern six centralised systems, but the Commission has indicated that: "Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the [interoperability] components."[31] The Council is also interested in this issue.[32] This would bring a lot more data on EU citizens into the picture (something that was also examined by the HLEG and subsequent studies[33]), but for the time being

30 Unless otherwise indicated, all references in this section to legislative provisions concern the two interoperability Regulations: Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0817; and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0818

31 European Commission, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems, COM(2017) 794 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:794:FIN

32 'Automating the exchange of police data: Council looks to national databases', *Statewatch News*, 9 September 2019, http://statewatch.org/news/2019/sep/eu-interop-national.htm

33 See, 'Registration of border crossings of EU citizens and other persons not covered by the Entry/Exit System' in the HLEG final report, May 2017, pp.23-25, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. A study carried out by the consultancy firm PWC for the European Commission subsequently examined the options set out in the final report in more detail, but for the time being it has been concluded that the focus should be on registering the movements of "persons of interest" in the SIS, rather than the wholesale collection of data on all border crossings by EU citizens.

the emphasis is on systems that principally exist to process the personal data of non-EU nationals.[34]

Despite this limitation, the changes introduced by the interoperability rules are significant. The six existing centralised databases noted above will now serve as building blocks: personal data will be extracted from them and used to construct new systems, with the aim of making the data accessible to a wider number of authorities than at present and using it in ways not initially foreseen in the legislation governing the underlying databases. Furthermore, a number of those databases have recently had their purposes extended (SIS), or are the subject of ongoing negotiations to do so (Eurodac and VIS), in particular with the aim of enhancing the ability of the authorities to expel people from EU territory.

The novel data processing operations introduced by the EU's interoperability initiative have led to criticisms that it undermines the key data protection principle of purpose limitation,[35] blurring – if not erasing – the lines between databases designed for distinct purposes, such as border control and law enforcement. Less than a decade ago, the introduction of the information architecture currently under construction would have been politically, legally and technically unthinkable. In 2010, a European Commission paper remarked:

> *"A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitute a gross and illegitimate restriction of individuals' right to privacy and data protection and pose huge challenges in terms of development and operation. In practice, policies in the area of freedom, security and justice have developed in an incremental manner, yielding a number of information systems and instruments of varying size, scope and purpose. The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative."*[36]

The argument put forward now is precisely the opposite – rather than recognising the value in separate, clearly-defined systems, the emphasis has switched to a more generalised use of the data available, focused around fixing a single digital identity to individuals.

According to the European Commission, "interoperability" is "the ability of information systems to exchange data and enable sharing of information." This "improves the efficiency and effectiveness of Europe-wide information-sharing tools, by ensuring the technical processes, standards and tools that allow EU information systems to work better together." It also means that "authorised users (such as police officers, migration officials and border guards) have faster, seamless and more systematic access to the information they need to do their jobs." It is argued that interoperability between the EU's databases will close "information gaps" and "blind spots" that hinder the work of the

34 Eurodac, the VIS, the EES and the ETIAS only process data on non-EU citizens. ECRIS-TCN will mainly process data on non-EU citizens, but some EU citizens who have dual nationality with a non-EU state will also be included in the system. The SIS can process data on both EU citizens and non-EU citizens.

35 The purpose limitation principle, as defined in Article 5(1)(b) of the General Data Protection Regulation, states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

36 European Commission, 'Overview of information management in the area of freedom, security and justice', COM(2010) 385 final, 20 July 2010, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/intro/docs/com_2010_385_en.pdf

authorities in combating crime, terrorism, identity fraud and irregular migration.[37]

The way in which this 'exchanging' and 'sharing' will take place has led to stern critiques. The chairs of the data protection bodies responsible for supervising three EU databases (Eurodac, SIS and VIS) described the Commission's use of the term "interoperability" as misleading, because the measures actually imply "the effective interconnection of the aforementioned information systems," which "could have a serious impact on key principles such as purpose limitation and proportionality."[38] A study conducted for the European Parliament argued that the Commission's proposals "do not establish a framework for interoperability, but instead propose technical solutions, some of which are compatible with the concept of interoperability, some of which are not."[39]

The Article 29 Working Party on Data Protection, meanwhile, lamented that "no analysis of less intrusive means to reach the goals set in these proposals [was] provided to justify the choices made."[40] The European Data Protection Supervisor remarked in their assessment of the proposals that making existing EU databases interoperable in the way foreseen "would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'."[41] The reasons for such concerns will be described in the sections that follow, with regard to each individual component of the EU's new "interoperable" information systems.

37 European Commission, 'Frequently asked questions - Interoperability of EU information systems for security, border and migration management', 12 December 2017, https://europa.eu/rapid/press-release_MEMO-17-5241_en.htm

38 '"Interoperability" proposals criticised again by EU data protection specialists', *Statewatch News Online*, 2 July 2018, http://www.statewatch.org/news/2018/jul/eu-interoperability-scg-letter.htm

39 Gutheil et. al., 'Interoperability of Justice and Home Affairs Information Systems', European Parliament Directorate General for Internal Policies, April 2018, p.13, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf

40 Article 29 Data Protection Working Party, 'Opinion on Commission proposals on establishing a framework for interoperability, 11 April 2018, http://www.statewatch.org/news/2018/apr/eu-art-29-wp-on-interop.pdf

41 European Data Protection Supervisor, 'Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems', 16 April 2018, https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

2.2. New systems

The interoperability rules introduce four new systems, which will make use of the data stored in the existing and new systems described in section 1, and in Annex 2 (SIS, Eurodac, VIS, EES, ETIAS and ECRIS-TCN):

- the **European Search Portal (ESP)**, which will make it possible to search through the six databases, as well as Interpol and Europol data, with a single click;
- the shared **Biometric Matching Service (BMS)**, which will extract biometric "templates" from each of the six EU databases, in order to simplify the searching and cross-matching of biometric data; and
- the **Common Identity Repository (CIR)**, containing the biometric and biographic identity data of hundreds of millions of non-EU nationals and, in certain cases, EU nationals,[42] extracted from Eurodac, the VIS, EES, ETIAS and ECRIS-TCN;
- the **Multiple-Identity Detector (MID)**, which will generate "identity confirmation files" to highlight matches between data stored in the CIR and the SIS;

Through a variety of means – such as "ensuring the correct identification of persons", "contributing to combating identity fraud", improving the quality of data in the underlying EU databases and "streamlining the conditions for access by law enforcement authorities to data held in the EES, ETIAS, VIS and Eurodac" – the new systems are supposed to achieve a variety of objectives:

- enhance the effectiveness and efficiency of border checks;
- contribute to preventing and combating irregular immigration;
- contribute to a high level of security within the EU;
- improve the implementation of the common visa policy;
- contribute to detecting, preventing and investigating terrorist and other serious criminal offences; and
- assist in identifying unknown persons or those unable to identify themselves (for example, following deaths in accidents or natural disasters).

42 ECRIS-TCN will primarily process data on non-EU citizens, but some EU citizens who have dual nationality with a non-EU state will also be included in the system. Their 'identity data' will thus also be transferred to the CIR. Legal experts have argued that the inclusion of dual nationals in ECRIS-TCN contravenes international non-discrimination law. See: Meijers Committee, 'ECRIS-TCN and the fundamental right to non-discrimination', https://www.commissie-meijers.nl/nl/comments/545

2.2.1. The European Search Portal (ESP)

Purpose

- facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems, to Europol data and to the Interpol databases for the performance of their tasks and in accordance with their access rights and the objectives and purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN[43]

The ESP will consist of "a central infrastructure, including a search portal enabling the simultaneous querying of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN as well as of Europol data and the Interpol databases," and secure communication channels between the ESP, national and EU authorities, and all other relevant databases and information systems that will be queried. It will be possible to conduct a search through the ESP with either alphanumeric or biometric data and, once it comes into use, it will become the default 'way in', for authorised users, to any of the databases and information systems to which it is connected.[44]

Access to the ESP will be given to national authorities or Union agencies with access to at least one of the six EU information systems summarised in section 1, to the CIR and the MID, to Europol data or to Interpol databases, with access governed by a variety of legal instruments.[45] It will be used by those authorities or agencies to query, simultaneously, all the databases and information systems that they are authorised to access, using either data on persons (i.e. biometric or biographic data) or their travel documents. It will also be used "to enable central systems to search other central systems," for example when the EES searches the VIS (to establish whether an individual crossing a border is a visa-holder) or the ETIAS searches other systems (to see whether data on an individual applying for a travel authorisation is held).[46] The authorities and agencies with access to the ESP must only use it and the data resulting from queries within it "for the purposes laid down in the legal instruments governing those EU information systems," the Europol Regulation and the interoperability Regulations.[47]

The ESP, which is essentially a unified search interface, is the least contentious element of the

43 Article 6

44 Article 7(2)

45 Article 7(1)

46 European Commission, Impact assessment accompanying the proposal for a Regulation of the European Parliament and of the Council establishing a framework for interoperability between EU information systems, SWD(2017) 473 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0473

47 Article 7(1)

interoperability initiative. Provided that user access rights are strictly defined and limited in accordance with the instruments governing each national or EU authority and the individual users within those authorities, it will merely speed up the process of searching databases and information systems to which access has already been granted. As the Regulations state: "the ESP shall query the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, Europol data and the Interpol databases simultaneously with the data submitted by the user and in accordance with the user profile."[48] Furthermore: "The ESP shall provide no information regarding data in EU information systems, Europol data and the Interpol databases to which the user has no access under the applicable Union and national law."[49]

However, the ESP is not entirely without its problematic elements. For example, it will be used to query Interpol's Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated With Notices (TDAWN) databases,[50] which are fed with information by that organisation's 194 member countries. When a search in these databases leads to a 'hit', the national authority that entered the alert is informed when, where and by whom the search was conducted. As highlighted by the Fundamental Rights Agency:

> *"regimes in third countries may manage to include an alert on one of their nationals or on a document held by that person in the Interpol database to prevent the person from travelling or to find out where the person is hiding."*[51]

The interoperability Regulations include a safeguard intended to prevent this happening: "Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert."[52] However, this is not something that can be controlled by the EU, as it requires changes to Interpol's Rules on the Processing of Data.[53] These are plans to reform these rules to "meet countries' needs and keep pace with developments," although the details of discussions, and whether they will encompass the requirements of the interoperability rules, are currently unknown.[54]

The introduction of the ESP and its ability to search across multiple databases at any one time may also make it more tempting to extend existing user access rights, giving officials permission to consult a greater number of databases than at present. Even without such any such extensions of access, the introduction of the ESP may make it easier for unscrupulous officials to misuse their existing permissions – for example, by allowing others to use their profile, or doing so on their behalf. The rules contain safeguards intended to prevent, or allow punishment of, such abuse,[55] but effective oversight and enforcement will require close scrutiny by national and European data protection authorities, which will have to be provided with the necessary resources.

48 Article 9(1)

49 Article 9(4)

50 Article 6(2)(a), Article 4(17)

51 'Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights', 11 April 2018, p.19, https://fra.europa.eu/en/opinion/2018/interoperability

52 Article 9(5)

53 In particular Article 104, 'Triggering of positive query results'. See: 'Interpol's Rules on the Processing of Data', https://www.interpol.int/content/download/5694/file/INTERPOL%20Rules%20on%20the%20Processing%20of%20Data-EN.pdf

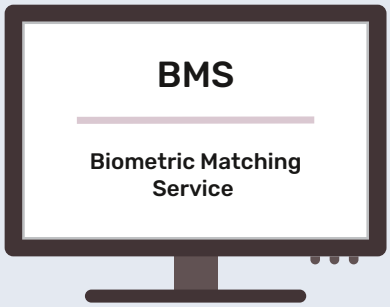
54 'INTERPOL reviews its rules for the international exchange of criminal data', *Interpol*, 22 March 2019, https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-reviews-its-rules-for-the-international-exchange-of-criminal-data. It appears that Jürgen Stock, the Secretary General of Interpol, was rather alarmed by the EU's plans to govern access to Interpol databases through the interoperability Regulations, rather than an agreement between the EU and Interpol. Nevertheless, his concerns were rebuffed by the Member States. See: 'Interoperability between EU information systems – Approval of a letter', Council of the EU document 7584/19, 22 March 2019, https://data.consilium.europa.eu/doc/document/ST-7584-2019-INIT/en/pdf

55 Article 10

2.2.2. The shared Biometric Matching Service (BMS)

Purposes

- supporting the CIR and the MID and the objectives of the EES, VIS, Eurodac, SIS and ECRIS-TCN



The shared Biometric Matching Service (BMS) will store biometric templates[56] from five of the six EU databases summarised in section 1 (biometric data is not gathered for the ETIAS). The system will be made up of "a central infrastructure, which shall replace the central systems of the EES, VIS, SIS, Eurodac and ECRIS-TCN respectively, to the extent that it shall store biometric templates and allow searches with biometric data," and a communications infrastructure between the BMS, CIR and the central database of the SIS.[57] That is to say, while facial images and fingerprints themselves will be retained in the underlying systems, templates generated from that data will be transferred to the BMS, which will be used for cross-matching and comparisons. A template cannot identify an individual, but does allow the identification of an individual if their biometric data matches templates in the BMS that correspond to data in one or more of the underlying systems.

The templates "shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the EU information systems," in order to ensure the data meets "a minimum data quality standard," which should reduce the possibility of false matches.[58] The types of biometric template and the systems from which they are extracted for storage in the BMS are shown in the table below.

56 A biometric template (also known as a search vector) is a mathematical representation of a biometric such as a fingerprint or facial image created through the extraction of certain points or features of that image. The image itself is discarded or, in this case, retained in the CIR. Section 8.2 of the Commission's impact assessment on the interoperability Regulations provides further explanation. See: SWD(2017) 473 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0473. See also: Ravi Das, 'What a Biometric Template is', *Biometric Update*, 28 November 2012, https://www.biometricupdate.com/201211/what-a-biometric-template-is

57 Article 12(1) and (2)

58 Article 13(3), Article 37(4): "The details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the EES, VIS, ETIAS, SIS, the shared BMS and the CIR, in particular regarding biometric data, shall be laid down in implementing acts." Implementation by the Member States must be reviewed annually by the Commission, which "shall make any necessary recommendations". Member States must then "provide the Commission with an action plan to remedy any deficiencies identified" (Article 37(5)).

Table 1: Biometric templates stored in the BMS

SIS	ECRIS-TCN	EES				VIS
		VISA-OBLIGED		VISA-EXEMPT		
		Permitted entry	Refused entry	Permitted entry	Refused entry	
photographs and facial images		facial image	facial image	facial image	facial image	
dactyloscopic data (excluding palm prints)	fingerprint data (ten fingers, including code of convicting MS)		fingerprints (four fingers) (if not registered in the VIS)	Fingerprints (four fingers)	fingerprints (four fingers)	fingerprints (ten fingers)

The purpose of the BMS is to enable "querying with biometric data across several EU information systems" in order to support the functioning of the CIR and the MID, as well as the objectives of the EES, VIS, Eurodac, SIS and ECRIS-TCN. Indeed, without a shared BMS, performing biometric matching through the CIR and MID would not be possible: "If biometric data were distributed over the various systems, every new addition of data would need to be searched against all other systems to detect the existence of data on the same person."59

Despite the technical purpose that it serves, however, it has been argued that: "The generation of biometric templates that are to be stored in the BMS constitutes a new data processing operation, for which the interoperability proposal does not provide a legal basis."[60] A further critique is that, given the utility of the BMS in detecting multiple identities across the five EU systems that use biometric data, it could have been implemented without the additional data processing required by the CIR and the MID.[61]

One question that has important implications for the BMS is whether biometric templates, rather than the biometric data on which those templates are based, constitute personal data.[62] If they do, then relevant EU and national law and jurisprudence on personal data protection applies to the processing of those templates.

An analysis of the interoperability proposals produced for the European Parliament argued that there is "ambiguity regarding the nature of templates," but that their storage in the BMS "essentially constitutes processing of personal data." Certainly, the creation of the templates in the first place requires the processing of personal data, as software must be used to extract templates from the images of fingerprints and faces. Beyond this point however, the Commission has argued that: "These templates alone, without the biometric data that originated them, do not allow

59 European Commission, Impact assessment, SWD(2017) 473 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0473

60 Teresa Quintel, 'Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention', 28 February 2018, p.16, https://orbilu.uni.lu/handle/10993/35318

61 Gutheil et. al., 'Interoperability of Justice and Home Affairs Information Systems', European Parliament Directorate General for Internal Policies, April 2018, p.13, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf

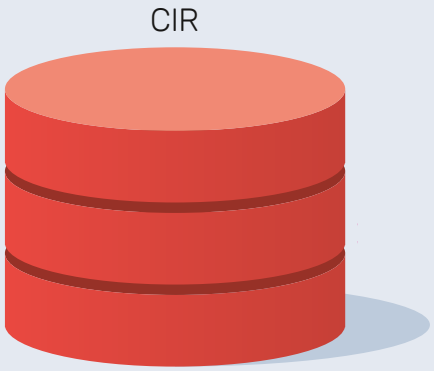
62 "Personal data" is defined in EU law as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". See: Article 4(1), General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

for the identification of a person,"[63] and they thus do not constitute personal data. While it may not currently be possible to identify an individual from a biometric template alone, whether it will remain so in light of technological developments remains to be seen, which may require a reassessment of the necessity and proportionality of the BMS.

2.2.3. The Common Identity Repository (CIR)

Purposes

- facilitating and assisting in the correct identification of persons
- supporting the functioning of the Multiple-Identity Detector (MID)
- facilitating and streamlining access by national authorities and Europol to the EES, VIS, ETIAS and Eurodac, where necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences[64]



63 European Commission, Impact assessment, SWD(2017) 473 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0473

64 Article 17

Table 2: Personal data held in the CIR[65]

Source	EES				ETIAS	VIS	ECRIS-TCN	Eurodac**
Data type	Visa-obliged		Visa-exempt					
	Entry	Refusal	Entry	Refusal				
Biometrics								
Fingerprints (number of prints)		•* (four)	• (four)	•* (four)		• (ten)	• (ten, including code of convicting Member State)	• (ten)
Facial image	•	•*	•	•*		•	Optional	•
Biographic data								
First name(s)	•	•	•	•	•	•	•	•
Surname	•	•	•	•	•	•	•	•
Former surname(s)						•		
Name at birth					•			•
Previous names							•	•
Previously used names								•
Aliases, pseudonyms, artistic names, usual names					•		•	•
Parents' first names					•			
Date of birth	•	•	•	•	•	•	•	•
Place of birth					•	•	•	•
Nationality(ies)	•	•	•	•	•		•	•
Sex	•		•	•	•	•		•
Gender							•	
Travel document data								
Type and number	•		•	•	•		•***	•
Issuing country code	•		•	•	•		•***	•
Validity	•		•	•	•		•***	•

* If the person is refused entry because of a false/counterfeit/forged travel document, visa or residence permit; or because they are subject to SIS or national alert on refusal of entry.

** Data from Eurodac will not be included until the proposed new Eurodac Regulation is approved. The categories listed here are those included in the interoperability proposals and the Eurodac proposal.

*** The interoperability Regulation refers to "information on travel documents". However, the ECRIS-TCN Regulation only refers to "identification documents".

65 Article 18

The CIR will be "a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN". It will be able to hold records on up to 300 million individuals and will "replace the central systems of respectively the EES, VIS, ETIAS, Eurodac and ECRIS-TCN," to the extent that it will store the data shown in the table above.[66] Information relating to the specific purposes of each system – for example, the times and dates of entry to and exit from the Schengen area (EES), whether a travel authorisation has been issued or not (ETIAS), or which Member State holds information on criminal convictions (ECRIS-TCN) – will remain in the individual systems.

As shown by the table above, the data in each file may vary slightly, depending on which database it has been extracted from in the first place. A reference in the individual files will indicate from which system the data is taken. In certain cases, it will come from more than one database (for example, data on visa-obliged non-EU nationals will come from both the EES and the VIS; files on visa-obliged and visa-exempt non-EU nationals with criminal convictions in the EU may also include data taken from the ECRIS-TCN). In short, however, every file will contain at least one biometric identifier and basic biographic data, in essence equivalent to that available in the chip of a biometric passport.

The first purpose of the CIR is "facilitating and assisting in the correct identification of persons." To this end, Article 20(1) of the interoperability Regulations permits "queries of the CIR" by "a police authority" conducting identity checks in various different circumstances. It is this particular aspect of the legislation that poses particular risks for the rights of undocumented migrants, because it makes available a vast new pool of data that may be accessible to a wide variety of authorities tasked with detecting persons in an irregular migration situation. These provisions, their (limited) safeguards and the implications are discussed further in section 3. The CIR may also be accessible to national authorities in the case of "a natural disaster, an accident or a terrorist attack and solely for the purpose of identifying unknown persons who are unable to identify themselves or unidentified human remains."[67] In such a case a police authority may also search the CIR, provided that it is subject to national legislation "laying down the procedures, conditions and criteria" for doing so.[68]

The second aim of the CIR is to support the functioning of the Multiple-Identity Detector, which is addressed in the following section. The third objective is to simplify access by national authorities and Europol to the EES, Eurodac, ETIAS and VIS, "where necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences." Any designated national authority or Europol can, "in a specific case, where there are reasonable grounds to be believe that consultation of EU information systems will contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences… consult the CIR," in order to see whether information is available in any of four of the systems (EES, Eurodac, ETIAS or VIS).[69]

An automated response will inform the searching authority which, if any, of those underlying systems contains matching data. A positive response "shall be used only for the purposes of submitting a request for full access subject to the conditions

66 Article 17

67 Article 20(4)

68 Article 20(6)

69 Article 22(1). In the case of Eurodac however, such searches will not be possible until negotiations on the new Eurodac Regulation are completed and the interoperability Regulations have also been amended to make possible the inclusion of Eurodac data in the CIR.

and procedures laid down in the legal instrument governing such access."[70] That is to say, if a search in the CIR returns a 'hit' regarding data originating from Eurodac, this "should not be interpreted or used as a ground or reason to draw conclusions on or undertake measures in respect of a person,"[71] and a request to access the full set of data stored in Eurodac would have to be launched in accordance with the rules governing that database. However, the interoperability Regulations are silent as to how compliance with this prohibition on drawing conclusions or undertaking measures may be ensured.[72]

As noted, the Regulations state that full access to the data held in the EES, Eurodac, ETIAS or VIS for law enforcement purposes "remains subject to the conditions and procedures laid down in the respective legal instruments governing such access." Recitals contained in the Commission's proposals that explicitly referred to abolishing the existing 'cascade' procedures did not make it into the final legislative text.[73] This procedure exists for Eurodac and the EES and obliges law enforcement authorities to search other potential sources of information (e.g. national criminal records or police fingerprint databases) before resorting to information gathered for non-policing purposes (e.g. the processing of asylum claims or border management). However, it is hard to see why these procedures would be maintained in light of those introduced for access to the CIR.

For example, in the case of the Entry/Exit System, the 'cascade' procedure requires a prior search in national databases and in the fingerprint databases of other Member States[74] (which can be searched via the technical infrastructure introduced by the 'Prüm' decisions[75]). But if an initial search in the CIR reveals that further information on an individual is held in the EES, what would be the point of going through the cascade procedure to obtain access to it?[76]

70 Article 22(2)

71 Recital 33

72 In their opinion on the interoperability proposals, the EDPS remarked: "facilitating the access by law enforcement authorities to non-law enforcement systems (even to limited information such as a hit/no hit) is far from insignificant from a fundamental rights perspective. One must bear in mind that those systems have been set up and developed in view of the application of specific policies and not as a law enforcement tool. Routine access would represent a violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of for instance travellers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted for that purpose. Moreover, removing genuine safeguards introduced to preserve fundamental rights mainly in the interest of speeding up a procedure would not be acceptable. If there is a need to improve the procedure, this should not be done at the expense of safeguards."

73 Recital 34 of the proposal said: "The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA should only cease to apply once the alternative safeguard of the two-step approach to law enforcement access through the CIR has become operational." See: Proposal for a Regulation, COM(2017) 794 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0794

74 Article 32, Regulation (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

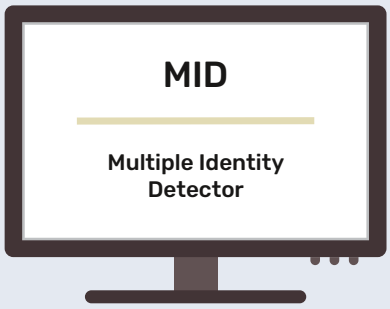
75 "The core of the Prüm framework lays down provisions under which EU Member States grant each other access to their automated DNA analysis files, automated fingerprint identification systems and vehicle registration data." See: European Commission, 'Prüm Decisions', https://ec.europa.eu/home-affairs/e-library/glossary/pr%C3%BCm-decisions_en

76 The issues raised by these changes are explained in more detail in section 3.3 of EDPS, 'Opinion 4/2018', pp.15-18, https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

2.2.4. The Multiple-Identity Detector (MID)

Purposes

- facilitate identity checks
- combat identity fraud
- support the functioning of the CIR and the objectives of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN



The high-level expert group on information systems and interoperability made no mention of a multiple-identity detector in its final report. Instead, the idea was introduced by the Commission in its legislative proposals and justified on the grounds that it was needed to overcome technical and financial barriers posed by the interoperability initiative.

Initially, there was an idea to move identity data stored in the SIS to the CIR, but this would have been both complex and expensive. In order to search through the biographic data stored in both the CIR and the SIS, the need for a new system was perceived:

> *"The multiple-identity detector would be this new technical component to check whether the biographical identity data contained in the search exists in any of the systems covered by the common identity repository (Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system) and in the SIS. This would enable the detection of multiple identities linked to the same set of biometric data, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud."*[77]

The MID will be activated whenever a new file is created or updated in the EES, VIS, or ETIAS, an alert on a person is created or updated in the SIS, or a new record is created or modified in the ECRIS-TCN.[78] It will make use of the BMS to compare biometric data across EU databases;[79] and the CIR and the SIS to do the same with biographic and travel document data.[80] Where there is a match between data in those systems and that in the file, alert or record that has been created, the MID will

77 European Commission, Impact assessment, SWD(2017) 473 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017SC0473

78 Article 27(1)(a)-(d). Provisions concerning Eurodac will be introduced once negotiations on the new Eurodac Regulation are complete.

79 Article 27(2)

80 Article 27(3)

generate an "identity confirmation file"[81] containing a "yellow link". This indicates that manual verification of the matching sets of data – generally by the authority that created the file, alert or record[82] – is required in order to determine how the matching data should be classified: as green, red, or white.

An official examining the two (or more) sets of data attached by a yellow link would be obliged to apply:

- a green link, when manual verification reveals that identical (or very similar) biographic identities have been detected, but they have different biometric data;[83]
- a red link, when multiple files contain the same biometric data, but different biographic data, and an official concludes that this is the result of identity fraud;[84] or
- a white link, when the same person exists in multiple systems (the same biometric data and the same, or very similar, biographic data in different files), or an investigation indicates that files hold the same biometric data but lawfully differing biographic data (for example, individuals who have changed their name or use an artistic persona).[85]
- A wide variety of authorities will be given access to identity data stored in the CIR and the SIS in order to carry out the process of identity verification. For example, were the creation of a file in the VIS to lead to the generation of a yellow link requiring manual verification, consular authorities would be given access to the identity data required for comparison and verification.[86] They would then have to "assess the different identities without delay" and, having done so, update the link accordingly and add it to the identity confirmation file.[87] Exactly how this assessment should be carried out, and on what basis different pieces of identity data may be considered the same or similar, will be defined in a delegated act to be adopted by the Commission.[88]

The application of green, red or white links to matching sets of identity data also gives rise to differing levels of access, for a variety of authorities, to identity data stored in the CIR and SIS and the related data stored in the MID.

- In the case of a **red link** – a presumption of identity fraud – the rules appear to contradict themselves. They state that any national authority or EU agency that has access to at least one EU information system included in the CIR, or to the SIS, shall have access to two of the components of the identity confirmation file in question: the red link itself and the reference to

81 Article 34 sets out the information contained in identity confirmation files: the links referred to in Articles 30 to 33 (yellow, green, red or white); a reference to the EU information systems in which the linked data are held; a single identification number allowing retrieval of the linked data from the corresponding EU information systems; the authority responsible for the manual verification of different identities; and the date of creation of the link or any update to it.

82 Particular rules exist in the case of certain types of SIS alerts: "For links obtained through SIS related to alerts in respect of persons wanted for arrest for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure or on persons for discreet checks, inquiry checks or specific checks, the authority responsible for the manual verification of different identities should be the SIRENE Bureau of the Member State that created the alert. These categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating data that are linked to them in one of the other EU information systems." See: Recital 44, Regulation (EU) 2019/817 and Regulation (EU) 2019/818

83 Article 31

84 Article 32

85 Article 33

86 Article 29(3); Article 21(1): "Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the manual verification of different identities in accordance with Article 29 shall have access, solely for the purpose of that verification, to the data referred to in Article 18(1) and (2) stored in the CIR connected by a yellow link."

87 Article 29(3)

88 Article 28(5)

the EU information systems in which the linked data is held.[89] On the other hand, they also state that: "Where the CIR or SIS are queried and where a red link exists between data in two or more of the EU information systems, the MID shall indicate the data [contained in the identity confirmation file]"[90] – that is, all the data contained in the file, rather than just two components. This article also makes clear that: "No legal consequence for the person concerned shall derive solely from the existence of a red link," and the authority applying a red link to linked identity data is required to inform the person concerned and provide information allowing them to take further action.[91]

- In the case of **white links**, access to the linked data will be granted to national authorities or EU agencies which "have access to the two EU information systems containing data between which the white link was created."[92] In the case of a query of the CIR or SIS indicating the existence of a white link, ""the MID shall indicate that the identity data of the linked data correspond to the same person." The underlying information systems will also "reply indicating, where relevant, all the linked data on the person… if the authority launching the query has access to the linked data under Union or national law."[93]

- National authorities or EU agencies will be given access to **green links** "where they have access to the two EU information systems containing data between which the green link was created and a query of those information systems has revealed a match with the two sets of linked data."[94] Following queries of the CIR or the SIS that indicate the existence of a green link, "the MID shall indicate that the identity data of the linked data do not correspond to the same person."[95]

It has been observed that the automated generation of yellow links by the MID will have more pronounced effects for certain groups of people – for example, those with common surnames, who have changed their name (in particular married women), or who have dual passports – because yellow links will be generated more frequently for these groups. They will thus be subject to more frequent checks and questioning.[96] It has also been highlighted that "comparisons of alphanumeric data will detect a great number of MID-links that need to be verified manually," which may "lead to disproportionate processing of personal data."[97]

Both these problems may be more pronounced for non-EU nationals (in particular those from countries using non-Latin alphabets, who will have transliterations of their names recorded in EU databases). Persons who possess no documentation may have particular difficulty ensuring their name is recorded correctly in a database. It is for this reason, of course, that EU initiatives

89 Article 26(2)

90 Article 32(2)

91 Article 32(4) and (5) require that the "person concerned" be provided with a standard form that informs them of "the presence of multiple unlawful identity data… the single identification number [that refers to the linked sets of data]… a reference to the authority responsible for the manual verification of different identities… and the website address of the web portal established in accordance with Article 49 of this Regulation," which is to be set up "for the purpose of facilitating the exercise of the rights of access to, rectification, erasure or restriction of processing of personal data."

92 Article 26(3)

93 Article 33(2)

94 Article 26(4)

95 Article 31(2)

96 FRA, op. cit., pp.36-37

97 Teresa Quintel, 'Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention', 28 February 2018, p.16, https://orbilu.uni.lu/handle/10993/35318

place such heavy emphasis on the processing of multiple biometric identifiers, which are less prone to duplication or error than alphanumeric data, but which also pose unique risks in terms of privacy and data protection.[98]

It is striking that no evidence was presented alongside the interoperability proposals to demonstrate that a new large-scale information system (the MID) is a justified response to the problem of identity fraud committed by non-EU nationals. The impact assessment accompanying the interoperability proposals stated that: "Detecting multiple identities is a key prerequisite in order for the EU central systems to achieve their respective purposes. Today, as a result of the silo approach… it is generally not possible to conduct cross-system identity checks." As if to illustrate the change in approach to the treatment of personal data in EU justice and home affairs databases that has emerged in recent years, the document argued that: "While this [silo] approach respects the differentiated purposes of the various systems it creates an unjustifiable information gap when it comes to the identification of a third-country national. As a result it indirectly protects those persons committing identity fraud."[99]

This may well be true, but it is unknown whether the scale of identity fraud amongst non-EU nationals within the EU is of a scale significant enough to justify the processing of the personal data of every single individual with a file in the SIS or CIR every time a new file, alert or record is created in an EU database. The workload this will generate is, however, expected to be significant. During a transitional period aimed at "dealing with the legacy data",[100] the ETIAS Central Unit (operated by Frontex) is responsible for carrying out multiple identity detection by comparing the biometric data stored in the EES, VIS, Eurodac and SIS. The transitional period will last for one year following a successful test of the MID but may be extended by a Commission delegated act for up to one further year.[101] Furthermore, it must be observed that using data gathered for one purpose – such as processing asylum claims (Eurodac) or establishing which Member State holds information on an individual's criminal convictions (ECRIS-TCN) – for the purpose of detecting multiple identities breaches the purpose limitation principle.[102]

98 Biometric data is a "special category" of personal data under EU data protection law. The threshold to justify its processing is thus higher than normal and it requires special protection when it is processed. See: Article 9, General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

99 Section 6.1.8.4, Impact assessment, SWD(2017) 473, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0473

100 'Presidency non-paper', Council document 8242/18, 27 April 2018, http://statewatch.org/news/2018/may/eu-council-interoperability-pres-non-paper-ees-red-links-frontex-8242-18.pdf

101 The process for the transitional period is set out in Article 69 of Regulation 2019/817 and Article 65 of Regulation 2019/818.

102 The EDPS particularly emphasised this point with regard to the ECRIS-TCN, the legal basis for which solely concerns judicial cooperation in criminal matters. See: EDPS, 'Opinion 4/2018', p.15, https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

3. Interoperability and undocumented migrants: fundamental rights and legal implications

The interoperability Regulations, the rules governing the six underlying EU databases, and the rules governing Europol (whose data is queried by the ESP) all contain specific data protection provisions intended to complement the more general data protection rules set out by the General Data Protection Regulation,[103] the Law Enforcement Directive,[104] and the Regulation on data protection in EU institutions, bodies and agencies.[105] The interoperability Regulations specify precisely how these pieces of legislation apply, while the recitals make clear their general spheres of application.[106]

In any case, all processing of personal data carried out within the EU must respect the seven basic data protection principles:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- data accuracy;
- storage limitation, i.e. limited retention of data;
- data integrity and confidentiality; and
- accountability (the ability of the data controller to demonstrate compliance with the six preceding principles).

Furthermore, the Court of Justice of the EU (CJEU) has established a set of standards that must be met by any EU law requiring the processing of personal data. These standards have now also been incorporated into the jurisprudence of the European Court of Human Rights (ECtHR) and they provide a useful lens to examine one of the most contentious aspects of the interoperability initiative – the possibility for national police authorities to conduct identity checks with the CIR.

103 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

104 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, https://eur-lex.europa.eu/eli/dir/2016/680/oj

105 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725

106 Recitals 53-57. In short: the Law Enforcement Directive applies to processing for law enforcement purposes and the GDPR for any other purposes, except where processing is carried out by EU institutions, agencies or bodies, in which case Regulation 2018/1725 applies, notwithstanding any more specific rules which may apply to national or Union bodies or agencies (such as Europol, whose data protection regime is set out in Regulation 2016/794).

3.1. Use of the CIR to conduct identity checks

When considering the rights of undocumented migrants, the most concerning aspect of the interoperability proposals is the introduction of the Common Identity Repository (CIR, described in section 2.2.3). This new database is intended to facilitate an increase in identity checks, making it easier to identify individuals who may no longer have the right to remain in the Schengen area. This is also the purpose of changes to the underlying databases and information systems that have either already been made (as with the SIS) or are under negotiation (such as Eurodac and the VIS), as explained in section 1. However, even if someone is not actually registered in the CIR, their absence will likely suggest to the authorities conducting an identity check that they are in an irregular situation.

As explained in section 2.2.3, the CIR will be "a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN". It will be able to hold records on up to 300 million individuals and will "replace the central systems of respectively the EES, VIS, ETIAS, Eurodac and ECRIS-TCN,"[107] to the extent that it will store identity data such as names, place and date of birth, nationality, as well as fingerprints and facial images.

Due to differences in the data gathered for the underlying systems, individual files in the CIR may vary slightly, but every file will contain at least one biometric identifier and basic biographic data, in essence equivalent to that available in the chip of a biometric passport. Information relating to the specific purposes of each system – for example, the times and dates of entry to and exit from the Schengen area (EES), whether a travel authorisation has been issued or not (ETIAS), or which Member State holds information on criminal convictions (ECRIS-TCN) – will remain in the individual systems and, in the case of identity checks, will only be available to authorities and individuals with permission to access the system in question.

107 Article 17, Regulation (EU) 2019/817 and Regulation (EU) 2019/818 (the interoperability Regulations). Unless otherwise specified, all references to legislative provisions in this section refer to these two Regulations.

3.2. Weak anti-discrimination safeguards

The interoperability legislation is extremely problematic given the broad, vague terminology used. For the purpose of "facilitating and assisting in the correct identification of persons," a "police authority" may query the CIR with the biometric[108] or alphanumeric[109] data of any person over the age of 12[110] in a number of different circumstances:

a. where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;
b. where there are doubts about the identity data provided by a person;
c. where there are doubts as to the authenticity of the travel document or another credible document provided by a person;
d. where there are doubts as to the identity of the holder of a travel document or of another credible document; or
e. where a person is unable or refuses to cooperate.

To be able to conduct these checks, an authority must be "empowered by national legislative measures," which are subject to two further criteria.

Firstly, they must "take into account the need to avoid any discrimination against third-country nationals."[111] The language is weak ("take into account the need") and there is no further detail on how such discrimination might or must be avoided. The legislation does state elsewhere that: "Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds"[112] – a welcome provision, but it does not address the fact that discrimination on prohibited grounds may take place before any personal data is processed for the purposes of the Regulation – for example, when a police officer 'selects' an individual in the street whom they wish to subject to an identity check. The concern here is that the mere availability of a vast new pool of data will encourage more identity checks (in particular of black and ethnic minority individuals, whether citizens of the EU or elsewhere) which would not otherwise be conducted, with no adequate safeguards against abuse. This is particularly so given the increasing use of mobile biometric devices by police forces across EU Member States, further easing the possibility of conducting biometric identity checks.

108 Article 20(2)

109 The EDPS criticised this approach, noting that identity checks usually involve a police authority requesting that an individual to prove their identity "by any appropriate means such as their identity card or any other valid document." The opinion argued that identity data should be taken first and biometric data only "as a last resort", as: "Taking systematically biometric data of a person during an identity check would create the risk of stigmatising certain people (or groups of people) based on their appearance and create unjustified difference of treatment between EU citizens and third country nationals." See: EDPS, Opinion 4/2018, p.14, https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

110 Article 20(1): queries of the CIR "shall not be allowed against minors under the age of 12 years old, unless in the best interests of the child."

111 Article 20(5)

112 Article 5: "Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly, persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration."

3.3. Unjustifiable targeting of non-EU nationals

The second criterion for the national legislative measures underpinning identity checks in accordance with Article 20 is that they "specify the precise purposes of the identification," within two of the objectives of the legislation: "contribute to the prevention and the combating of illegal immigration";[113] and "contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding security in the territories of the Member States."[114] While these have both been recognised as objectives of general interest by the CJEU and ECtHR, the lack of specificity provided in the legislation does not appear to be in line with European jurisprudence.

In *Digital Rights Ireland*,[115] the CJEU examined the compatibility of the fundamental rights to privacy and data protection with the Data Retention Directive,[116] a law enforcement measure that required the retention of "all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony," in case it should later be required in criminal investigations. In a judgment that annulled the Directive and sparked a series of ongoing disputes over national data retention regimes, the court laid down a series of principles to determine the legitimacy of data processing measures that have since been accepted into the case-law of both the CJEU[117] and the ECtHR.[118]

The court noted that the broad scope of retention required by the Directive entailed "an interference with the fundamental rights of practically the entire European population."[119] The scope of the CIR is clearly not as expansive, as it overwhelmingly affects third-country nationals,[120] the majority of whom will be present in the EU.[121] Furthermore, their data is not arbitrarily included in the CIR, but is initially gathered on the basis of the legislation establishing each individual system (although some have called into question the compatibility

113 Article 2(1)(b)

114 Article 2(1)(c)

115 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland/Kärntner Landesregierung and others*, 8 April 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

116 The Directive was annulled by the CJEU, although national data retention schemes remain in place in numerous EU Member States: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024

117 Case C-362/.14, *Schrems*, 6 October 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362; Joined Cases C-203/15 and C-698/15, *Tele2/Watson*, 21 December 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203; Case Opinion 1/15, *Opinion of Advocate General Mengozzi*, 8 September 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CC0001

118 *Big Brother Watch and others v the United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 13 September 2018, http://hudoc.echr.coe.int/eng?i=001-186048

119 Para. 56, *Digital Rights Ireland*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

120 The only data on EU nationals that will be present in the CIR concerns dual nationals holding both EU and non-EU citizenship who have received a criminal conviction in an EU Member State, extracted from the ECRIS-TCN.

121 The EES, ETIAS and VIS store information on persons refused entry, refused a travel authorisation or refused a visa and thus cannot enter the Schengen area. Files in the EES and ETIAS are also retained once individuals leave the Schengen area, while the SIS stores data on entry bans, the majority of which refer to persons who have been expelled from the EU.

of aspects of these systems with CJEU jurisprudence[122] and international law[123]).

Nevertheless, one of the reasons that led the CJEU to annul the Data Retention Directive was that it "applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime." [124]

The CIR may be used for identity checks not just on the grounds of "combating illegal immigration", but also for contributing to "a high level of security". The presumption that individuals travelling to the EU from elsewhere in the world should be subject to controls of one kind or another – for example, for the purpose of obtaining a visa – is one that would be broadly accepted. However, this does not mean it is necessarily legitimate to use that same data for purposes other than those for which it was initially collected.

Given that there is no evidence to suggest that non-EU nationals are more likely than EU nationals to be engaged in activities threatening to "public security or public policy", the proportionality of this aspect of the legislation is questionable. The European Data Protection Supervisor commented on this point in their opinion on the proposals, suggesting that:

> *"access to the CIR to establish the identity of a third country national for purposes of ensuring a high level of security should only be allowed where access for the same purposes to similar national databases (e.g. register of nationals/residents) exist and under equivalent conditions… Otherwise, the Proposals would clearly seem to establish a presumption that third country nationals constitute by definition a security threat."*[125]

Given that the Regulations do not require any such conditions be laid down by the Member States in the national measures governing access to the CIR, it remains to be seen whether implementing legislation will include such safeguards. This is something that will require close scrutiny at national level.

122 Dr Mark D. Cole and Teresa Quintel, 'Data Retention under the Proposal for an EU Entry/Exit System (EES): Analysis of the impact on and limitations for the EES by *Opinion 1/15* on the EU/Canada PNR Agreement of the Court of Justice of the European Union', October 2017, Greens/European Free Alliance, https://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF. See also: 'Massive biometric 'smart borders' database may be illegal', *Statewatch News Online*, 15 September 2017, http://statewatch.org/news/2017/sep/cjeu-pnr-ees.htm

123 Letter from the Meijers Committee to Claude Moraes MEP, 'The fundamental right to non-discrimination', 22 January 2019, https://www.commissie-meijers.nl/sites/all/files/cm1902_ecris-tcn_and_the_fundamental_right_to_non-discrimination_0.pdf

124 Para. 58, *Digital Rights Ireland*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

125 EDPS, Opinion 4/2018, p.14, https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

3.4. No strict limits on access to data

The Data Retention Directive was also condemned by the CJEU for failing to "lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions," instead simply referring to "serious crime, as defined by each Member State in its national law."[126] While "serious crime" at least suggests a certain threshold, the interoperability Regulations merely establish a set of five possible circumstances and require that when such a circumstance arises, action be taken in accordance with national law and for some purpose falling within those two broad objectives outlined above. In short, the rules are not subject to the necessary specifications and restrictions that might make it possible to justify an interference with individual rights.

The court also noted that the Data Retention Directive did "not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use." Article 4 of the Directive stated: "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law" and required that such access be "in accordance with necessity and proportionality requirements" and subject to "the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."

The court found this article to be insufficient, noting that it:

> *"does not expressly provide that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements."*[127]

In the case of identity checks conducted using the CIR, there is no precise definition of any particular offences, the suspicion of which may be sufficient to permit access to the personal data within the system. Furthermore, as with the Data Retention Directive, it is left to the Member States to "define the procedures to be followed and the conditions to be fulfilled," which does not meet the requirement for EU law to lay down specific and precise measures concerning the processing of personal data.

126 Para. 60, *Digital Rights Ireland*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

127 Para. 61, *Digital Rights Ireland*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

3.5. Potential to undermine 'firewalls'

The legislation also gives rise to a further concern which may specifically affect undocumented migrants, although the potential situations in question are dependent on national implementation of both the interoperability rules and EU legislation on data protection.

The interoperability legislation states that identity checks conducted in accordance with Article 20 must be carried out by "a police authority", which is defined with reference to the Directive on data protection in law enforcement.[128] However, Member States have some room to interpret the provisions of the Directive as they see fit. For example, according to the UK's Data Protection Act 2018, a competent authority is as defined in the Directive, but may also be "any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes."[129] Law enforcement purposes is defined as "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

In Member States where irregular entry and/or stay is subject to criminal (rather than administrative) punishment,[130] an extremely wide variety of authorities could be given access to the CIR for carrying out identity checks. It is only necessary to consider some of the measures employed as part of the UK's 'hostile environment' – requiring identity checks for immigration purposes by landlords, health services and banks, for example[131] – to see how such a scenario might arise.

The national implementation of the interoperability Regulations will require close scrutiny to observe if and how it complies with fundamental rights requirements. The CIR will provide a vast pool of new data which may be used by police authorities to conduct identity checks for extremely broad purposes. The interoperability legislation does not establish sufficient anti-discrimination safeguards, nor does it set out the precise rules to govern the scope and application of the measure in question, as required by the jurisprudence of the CJEU and the ECtHR. A further concern arises in relation to the way in which national implementation of the Directive on data protection in law enforcement may interact with the interoperability rules, potentially providing a vast swathe of authorities with access to the CIR for identity checks.

It must be borne in mind that the interoperability proposals were introduced whilst many of the rules governing the existing databases were being rewritten, primarily with the aim of expanding their purposes to facilitate expulsions. The scope of the new 'interoperable' databases is thus potentially subject to change whenever one of the underlying systems is altered. If the reform of Eurodac results in the changes proposed, it will introduce centralised storage of data on persons found to

128 Article 4(19) of the interoperability Regulations states: "'police authority' means the competent authority as defined in point (7) of Article 3 of Directive (EU) 2016/680". Directive 2016/680 defines "competent authority" as: "(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

129 Article 30(1)(b), Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12

130 Fundamental Rights Agency, 'EU Member States' legislation on irregular entry and stay, as well as facilitation of irregular entry and stay', https://fra.europa.eu/sites/default/files/fra-2014-criminalisation-of-migrants-annex_en.pdf

131 Jamie Grierson, 'Hostile environment: anatomy of a policy disaster', *The Guardian*, 27 August 2018, https://www.theguardian.com/uk-news/2018/aug/27/hostile-environment-anatomy-of-a-policy-disaster

be irregularly staying in the Member States and the addition of their identity data to the CIR. Advocates of the rights of undocumented migrants should thus give particular consideration to the details of the ongoing discussions on the Eurodac proposal.

Beyond these immediate concerns, the future direction of personal data processing at EU level must also be taken into consideration. As remarked in section 2.1, the new architecture of EU databases and information systems introduced by both the interoperability Regulations and the reconfiguration of the underlying systems would have been technically, politically and legally unthinkable just a decade ago. There is already a clear intention to consider bringing other databases and information systems, many of which are principally concerned with EU citizens rather than 'third-country nationals', into the scope of the interoperability initiative. The question which must then be asked is, given ongoing political, social and technological developments, what might this architecture look like a decade from now, and what implications might it have for the fundamental rights of everyone living in the EU?

Annex 1: Objectives, Legal Bases and Legislation

1. Existing systems

	Purposes	Legal basis	Legislation
Eurodac	Determining Member State responsible for examining an application for international protection and otherwise facilitating application of the 'Dublin' rules Contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences Proposed: assist with control of irregular immigration to and secondary movements within the Union and with identification of irregularly staying third-country nationals	Ensure a high level of security within the area of freedom, security and justice of the Union and ensure application of TFEU provisions on movement of persons within Member States' territory	Regulation (EU) No 603/2013[132] Proposed: Regulation on the establishment of 'Eurodac' (recast)[133]
SIS	Ensure a high level of security within the area of freedom, security and justice of the Union and ensure application of TFEU provisions on movement of persons within Member States' territory	Article 62(2)(b)(ii) TEC Article 66 TEC Proposed: Article 16(2) TFEU Proposed: Article 77(2)(a), (b), (d), (e) TFEU Proposed: Article 78(2)(d), (e) TFEU Proposed: Article 79(2)(c), (d) TFEU Proposed: Article 87(2)(a) TFEU Proposed: Article 88(2)(a) TFEU	Regulation (EU) 2018/1860[134] Regulation (EU) 2018/1861[135] Regulation (EU) 2018/1862[136]

132 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603

133 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272

134 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1860

135 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1861

136 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019PC0004

	Purposes	Legal basis	Legislation
VIS	Facilitate the visa application procedure Prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application Facilitate the fight against fraud Facilitate checks at external border crossing points and within the territory of the Member States Assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States Facilitate the application of the Dublin Regulation Contribute to the prevention of threats to the internal security of any of the Member States Proposed: assist in the identification of persons who have gone missing Proposed: facilitate the application of the Dublin Regulation and asylum procedures Directive Proposed: contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences Proposed: ensure the correct identification of persons	Article 62(2)(b)(ii) TEC Article 66 TEC Proposed: Article 16(2) TFEU Proposed: Article 77(2)(a), (b), (d), (e) TFEU Proposed: Article 78(2)(d), (e) TFEU Proposed: Article 79(2)(c), (d) TFEU Proposed: Article 87(2)(a) TFEU Proposed: Article 88(2)(a) TFEU	Regulation (EC) No 767/2008[137] Council Decision 2008/633/JHA[138] Proposed: Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA[139]
EES	Enhance the efficiency of border checks by calculating and monitoring the duration of the authorised stay of third-country nationals admitted for a short stay Assist in the identification of third-country nationals who do not or no longer fulfil the conditions for entry to, or for short stay on, the territory of the Member States Allow the identification and detection of people who have overstayed their visa Allow refusals of entry in the EES to be checked electronically Enable automation of border checks on third-country nationals Enable visa authorities to have access to information on the lawful use of previous visas Inform third-country nationals of the duration of their authorised stay Gather statistics on the entries and exits, refusals of entry and overstays of third-country nationals Combat identity fraud and the misuse of travel documents	Article 77(2)(b), (d) TFEU Article 87(2)(a) TFEU	Regulation (EU) 2017/2226[140]

137 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019PC0004

138 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008D0633

139 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

140 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

	Purposes	Legal basis	Legislation
ETIAS	Assessing whether a third-country national exempt from visa requirements would pose a security, irregular immigration or high epidemic risk Enhance the effectiveness of border checks Support the objectives of SIS Contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences	Article 77(2)(b), (d) TFEU Article 87(2)(a) TFEU	Regulation (EU) 2018/1240[141]
ECRIS-TCN	Identifying EU Member State(s) where criminal convictions have been handed down against non-EU nationals and stateless persons	Article 82(1)(d) TFEU	Regulation (EU) 2019/816[142] Directive (EU) 2019/884[143]

2. Interoperability

	Interoperability Regulations
Purposes	enhance the effectiveness and efficiency of border checks to contribute to preventing and combating "illegal immigration" to contribute to a high level of security within the EU to improve the implementation of the common visa policy to contribute to detecting, preventing and investigating terrorist and other serious criminal offences to assist in identifying unknown persons or those unable to identify themselves (for example, following deaths in accidents or natural disasters)
Legal basis	Article 16(2) Article 74 Article 77(2)(a), (b), (d) and (e) Article 78(2)(e) Article 79(2)(c) Article 82(1)(d) Article 85(1) Article 87(2)(a) Article 88(2)(a)
Legislation	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa[144] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration[145]

141 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

142 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0816

143 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0884

144 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817

145 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0818

3. Relevant treaty provisions

Treaty on the Functioning of the European Union

Title II: Provisions having general application

- Article 16(2): Parliament and Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, by the Member States when implementing Union law, and rules on the free movement of such data

Title V: Area of freedom, security and justice

Chapter 1: General provisions

- Article 74: Council shall adopt measures to ensure administrative cooperation between the relevant departments of the Member States in the areas covered by this Title, as well as between those departments and the Commission

Chapter 2: Policies on border checks, asylum and immigration

- Article 77(2)(a): adoption of measures on visas and short-stay residence permits
- Article 77(2)(b): checks on persons crossing external borders
- Article 77(2)(d): establishment of an integrated external border management system
- Article 78(2)(d): common procedures for the granting and withdrawing of uniform asylum or subsidiary protection status
- Article 78(2)(e): criteria and mechanisms for determining which Member State is responsible for considering an application for asylum or subsidiary protection
- Article 79(2)(c): irregular immigration and unauthorised residence, including removal and repatriation of persons residing without authorisation
- Article 79(2)(d): combating trafficking in persons, in particular women and children
- Article 78(2)(e): criteria and mechanisms for determining which Member State is responsible for considering an application for asylum or subsidiary protection
- Article 79(2)(c): irregular immigration and unauthorised residence, including removal and repatriation of persons residing without authorisation

Chapter 4: Judicial cooperation in criminal matters

- Article 82(1)(d): judicial cooperation in criminal proceedings and enforcement of decisions
- Article 85(1): Eurojust

Chapter 5: Police cooperation

- Article 87(2)(a): collection, storage, processing, analysis and exchange of relevant information
- Article 88(2)(a): Europol - the collection, storage, processing, analysis and exchange of information

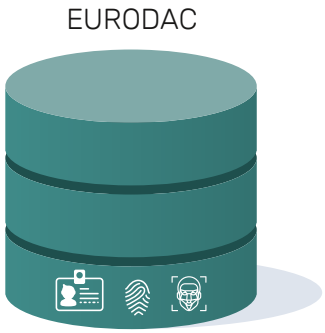
Treaty establishing the European Community

Title IV: Visas, asylum, immigration and other policies related to free movement of persons

- Article 62(2)(b)(ii) TEC, measures on the crossing of external borders: procedures and conditions for Member States to issue short-stay visas
- Article 66: measures to ensure administrative cooperation between the relevant departments of the Member States in the areas covered by this Title, as well as between those departments and the Commission

Annex 2: Additional Information on Existing Systems

1. Eurodac



In December 2000 the Council of the EU established Eurodac, a database to store the fingerprints of asylum seekers (known as 'Category 1') and individuals apprehended in connection with irregular border-crossings ('Category 2'), with the aim of facilitating the 'Dublin' rules on determining the Member State responsible for processing applications for international protection. Capturing and comparing fingerprints makes it possible for national authorities to determine whether another Member State should be responsible for handling an individual's application. Fingerprints can also be taken from third-country nationals or stateless persons found irregularly staying in a Member State ('Category 3'), but these are not currently stored in the central database. Instead, they are compared to the other datasets to establish whether an individual has previously applied for asylum or irregularly crossed an external border. In 2013, new rules made it possible for law enforcement authorities to access the system under certain conditions.

In the midst of the 'refugee crisis' in May 2016, a number of changes to the system were proposed by the European Commission.[146] This new Regulation, which is still under negotiation, would extend data retention periods for individuals falling within Category 2 from 18 months to five years.[147] In a change with particular impact for undocumented migrants, Category 3 data would go from merely being compared with data in the Central System to being stored for five years,[148] with the aim of assisting national authorities in "identifying illegally staying third-country nationals on their territory for return purposes" and potentially providing "precious elements of evidence for re-documentation and readmission purposes."[149] According to the proposal, the retention period for Category 1 data would remain the same at 10 years.[150] However, the age limit for all three categories would be significantly lowered (from 14 to six), significantly expanding the scale of data collection. As now, this data would also be available to national law enforcement authorities and Europol under the conditions explained below.

Under the proposal, new types of data would also be added to the Central System, which currently only holds fingerprints and other administrative information such as the date and time at which they were taken. If the changes proposed by the

146 Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES), COM(2016) 194 final, 6 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0194

147 Ibid.

148 Ibid.

149 Ibid.

150 Ibid.

Commission are approved by the Council and Parliament, a uniform set of identity data would be transmitted to the Central System for each category, including two biometrics (fingerprints and a facial image) and biographic data such as names, place and date of birth and nationality (see Figure 3 for an overview of the current situation and proposed changes).

The primary users of Eurodac are national migration and asylum authorities.[151] However, as noted, law enforcement agencies and Europol may also access the system under certain conditions. A reasoned request must be made to the relevant National Access Point which demonstrates that the comparison of fingerprint data with the Eurodac database is (1) necessary for "the prevention, detection or investigation of terrorist offences or of other serious criminal offences";[152] (2) concerns a specific case; and (3) "there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question."[153] Searches of other databases must also have been carried out through the 'cascade' procedure (introduced as a safeguard in what was an extremely controversial proposal), but it appears this will be abolished by the interoperability rules, as explained in section 2.2.3.[154] Through this procedure, authorities must have searched national fingerprint databases; other Member States' fingerprint databases; and the Visa Information System (VIS) without success before turning to Eurodac. Law enforcement access is maintained in the new Eurodac proposal, which may also provide the possibility for searches using facial images.[155] However, negotiations on the proposal are ongoing.

151 eu-Lisa, 'List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Article 27(2) of the Regulation (EU) No 603/2013, for the purpose laid down in Article 1(1) of the same Regulation', April 2019, https://www.eulisa.europa.eu/Publications/Reports/2019%20Eurodac%20updated%20list%20of%20authorities%20-%20asylum.pdf

152 "Serious criminal offence" is defined in the Regulation as "the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA [the European Arrest Warrant], if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years," while "terrorist offences" are "the offences under national law which correspond or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA [the Directive on combating terrorism, now replaced by Directive 2017/541]."

153 Article 21(c), Regulation (EU) No 603/2013.

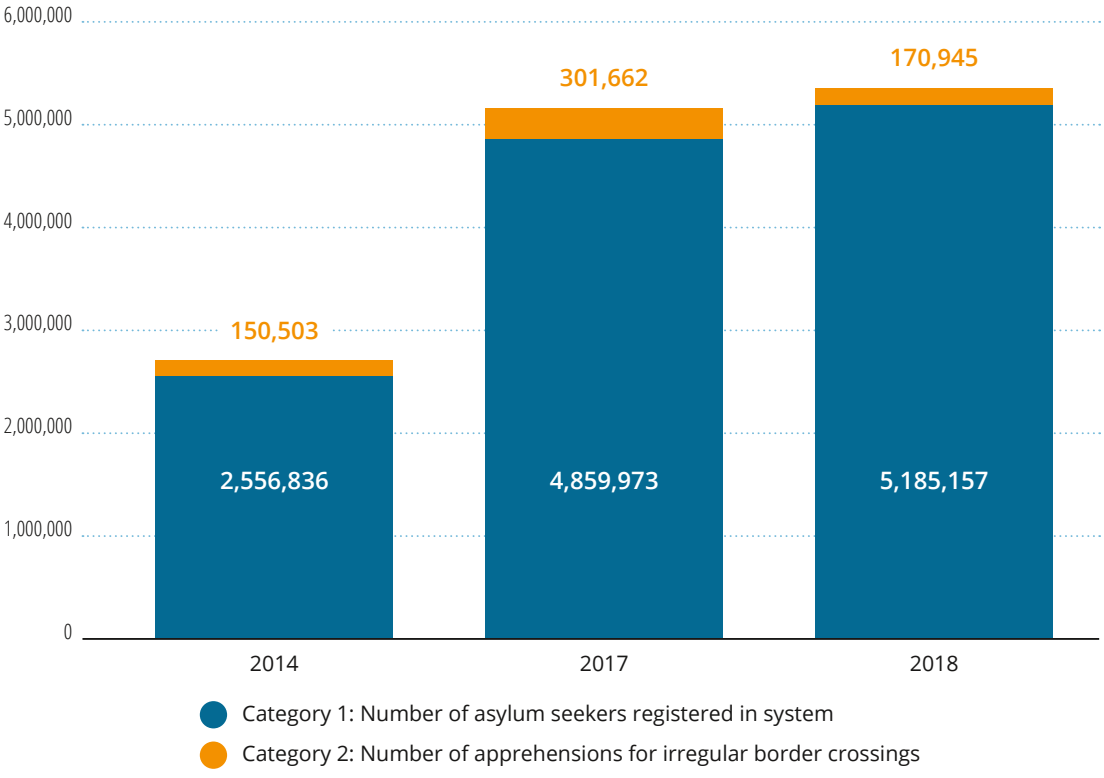
154 Data protection and refugee rights experts warned that making Eurodac available to law enforcement authorities would have a stigmatising effect upon asylum-seekers and irregular migrants as a group by associating them with criminal activity. The UNHCR remarked that: "People registered in Eurodac with no criminal record would face greater likelihood of being subject to criminal investigation than other members of the community whose fingerprints are not collected or stored on a systematic basis." See: 'European Parliament's Civil Liberties Committee adopts proposal giving law enforcement authorities and Europol access to Eurodac', *Statewatch News Online*, 19 December 2012, http://database.statewatch.org/article.asp?aid=32044

155 Article 20(3), Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac', COM(2016) 272 final 2016/132 (COD), 4 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272

Figure 3: Data captured and retained in the Eurodac Central System

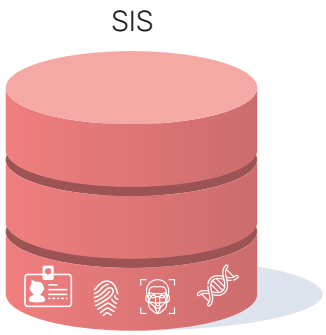
	Category 1	Category 2	Category 3
Data captured (current Regulation) (2016 proposal)	Fingerprints (Fingerprints; Facial image; Surname(s), forename(s), name(s) at birth, previously used names and aliases; Nationality(ies); Place/date of birth; Member State of origin; Place and date of application; Sex; Type and number of travel document, three-letter country code and validity period)	Fingerprints (Fingerprints; Facial image; Surname(s), forename(s), name(s) at birth, previously used names and aliases; Nationality(ies); Place/date of birth; Member State of origin; Place and date of apprehension; Sex; Type and number of travel document, three-letter country code and validity period)	Fingerprints (Fingerprints; Facial image; Surname(s), forename(s), name(s) at birth, previously used names and aliases; Nationality(ies); Place/date of birth; Member State of origin; Place and date of apprehension; Sex; Type and number of travel document, three-letter country code and validity period)
Data retention (current Regulation) (2016 proposal)	Ten years (ten years)	18 months (five years)	Data not stored, just compared to check for previous asylum application(s) (five years)
Age limit (current Regulation) (2016 proposal)	14+ (6+)	14+ (6+)	14+ (6+)

Figure 4: Eurodac Central System, 2014-18



Source: eu-Lisa. Data is unavailable for 2015 and 2016

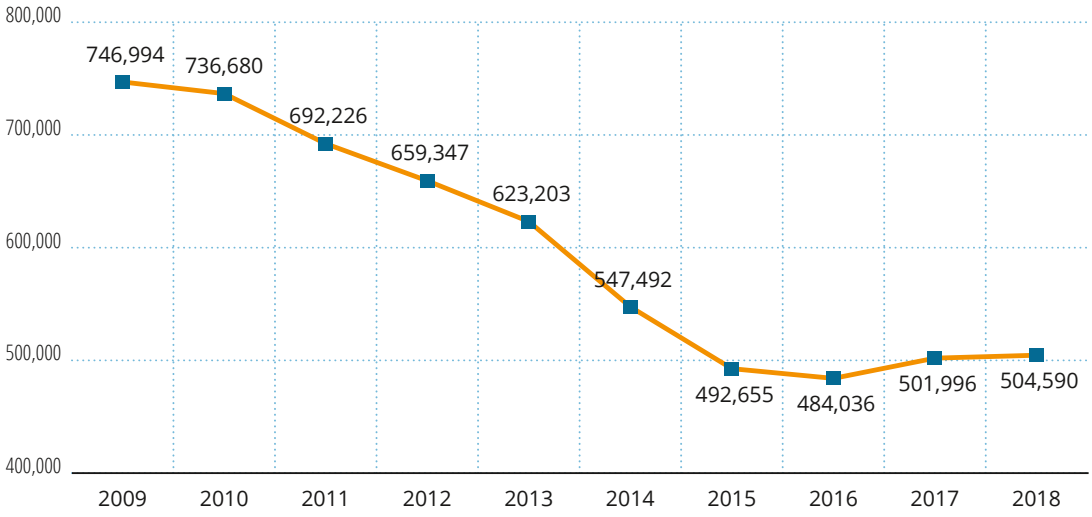
2. Schengen Information System (SIS)



The SIS II is the world's largest law enforcement database and under new legislation agreed in 2018 is set to get even larger. It contains millions of alerts on missing and stolen objects, wanted persons, individuals subject to discreet surveillance and checks, and individuals barred from entering the Schengen area. One key aim of the new rules is to beef up the system's role in enforcing return orders and entry bans, with the aim of ensuring the expulsion of more irregular migrants and preventing their re-entry to the Schengen area. It will now become mandatory for all Member States to insert information on return decisions and their enforcement into the SIS, something that was previously dependent on national law. The expanded use of entry bans has been introduced by changes to the SIS legislation and further changes are under discussion in the context of amendments to the Returns Directive. The number of individuals subject to alerts on refusal of entry or stay declined significantly from 2009 to 2015, when it began rising again. It is likely that the number of such alerts will increase more sharply in the coming years.

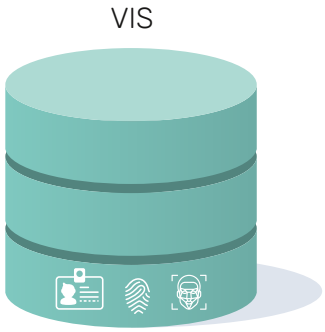
The principal users of the SIS for return purposes and border checks are national migration and asylum authorities, although due to the system's multi-purpose nature a wide array of bodies and agencies currently have access to varying sets of information. Frontex staff will be provided with access to the database in the context of return operations and when they are deployed to conduct border checks.

Figure 5: Alerts on refusal of entry or stay



Source: eu-Lisa/Council of the EU

3. Visa Information System (VIS)



The Visa Information System (VIS) is a large-scale database that first came into use in October 2011 and was fully deployed by the end of 2015. It is currently used to store information on all applications for short-stay Schengen visas. A central database managed by eu-Lisa is connected to national systems, including in Member States' consulates and other locations where visa applications are processed. The system also has the capability to match biometrics: "primarily of fingerprints, for identification and verification purposes."[156] These are gathered as part of the visa application process from all applicants aged 12 or over. The system was first used in Member States' consulates and embassies in North Africa and by October 2015 was in use across the world.[157]

One of the current objectives of the VIS is "to assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States." This may be done at border crossing points or within EU territory to examine "whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled."[158] In May 2018 the European Commission published a proposal to alter the system in a number of ways,[159] including so that it can "assist in the process of identifying and returning any person who may not or no longer fulfil the conditions for entry to, stay or residence in the Member States" (emphasis added).[160]

As with the other databases already discussed, national authorities are the main users, principally those responsible for processing visa applications and border control agencies. In the context of the visa application procedure, private companies may also have access.[161] National law enforcement agencies and Europol can access the database for criminal investigations, under certain conditions. In the case of national authorities, access (1) "must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences; (2) "must be necessary in a specific case"; and (3) there must be "reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question."[162] For Europol, access is possible "when necessary for the

156 European Commission, 'Visa Information System (VIS)', https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en

157 European Commission, 'Visa Information System now fully operational worldwide', 2 December 2015, https://ec.europa.eu/home-affairs/what-is-new/news/news/2015/20151202_2_en

158 Article 20, Regulation 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0767

159 The new proposal also requires the central storage of some data on holders of long-stay visas and residence permits (whose issuance is a national competence) and in doing so introduces a requirement to take biometric data from those individuals. Further controversial aspects of the proposals include profiling and, as with Eurodac, lowering the fingerprinting age to six years old. See: 'Visa Information System: Commission proposals sneak in mandatory biometrics for long-stay visas', *Statewatch News Online*, 20 August 2018, http://www.statewatch.org/news/2018/aug/vis-fingerprints-long-stay-visas.htm; 'All visa applicants to be profiled and children fingerprinted for revamped Visa Information System', *Statewatch News Online*, 17 August 2018; 'Visa Information System: child fingerprinting and police access proposals criticised by data protection authorities', *Statewatch News Online*, 21 January 2019, http://www.statewatch.org/news/2019/jan/eu-vis-scg-letter.htm

160 European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, COM(2018) 302 final, 16 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

161 'Visa Information System: private companies gathering data, insufficient funding for data protection', *Statewatch News Online*, November 2015, http://database.statewatch.org/article.asp?aid=35780

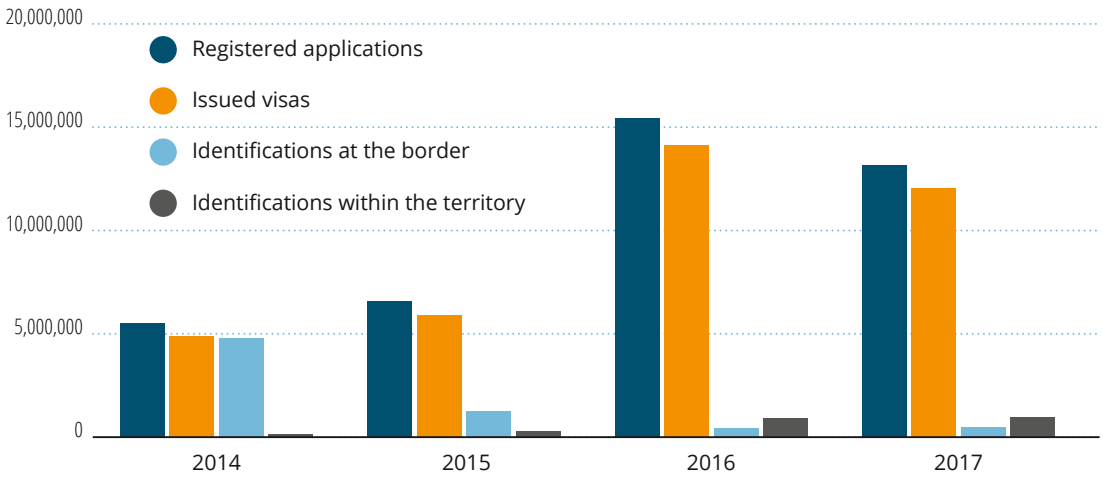
162 Article 5(1), Council Decision 2008/633/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0633

performance of its tasks... and for the purposes of a specific analysis" or "for an analysis of a general nature and of a strategic type".[163] In both cases, requests must be made to a designated central access point and searches are only possible with certain types of information,[164] although a successful search will return further types of data as well.[165] In contrast to Eurodac and the EES, there is no 'cascade' procedure for law enforcement access to the VIS.

Under the proposed new Regulation, Frontex officials will also be given access to the VIS under certain conditions. They can do so when carrying out border checks; to verify whether an individual fulfils the conditions for entry, stay or residence in a Member State; and when "identifying any person that may not or may no longer fulfil" those conditions,[166] the latter point being particularly relevant in the context of return proceedings.

According to the proposal, Frontex officials will require authorisation from their host Member State to conduct searches, although it is unclear how the "host" condition will apply in the context of deportations coordinated from Frontex's office in Warsaw. The agency will have to establish a "central access point", through which Frontex officials will have to make requests to access the system, which makes it appear as if the agency will ultimately authorise itself[167] (a similar process applies for access by Europol to EU databases[168]). At the same time, however, "staff involved in return-related tasks may only act in response to information obtained from the VIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating."[169]

Figure 6: Visa applications and identifications 2014-2017



163 Article 7(1), Council Decision 2008/633/JHA

164 Article 5(2), Council Decision 2008/633/JHA

165 Article 5(3), Council Decision 2008/633/JHA

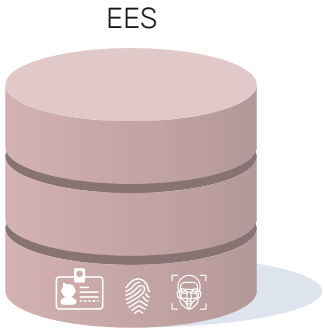
166 Article 45d and 45e(5), COM(2018) 302 final, 16 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

167 Article 45e(1), COM(2018) 302 final

168 See, for example, Article 30, Regulation (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226#d1e2809-20-1;

169 Article 45e(3)

4. Entry/Exit System (EES)



The Entry/Exit System (EES) will be used to monitor the cross-border movements of temporary visitors to the Schengen area and to automatically calculate the amount of time they are permitted to stay. In doing so, it will replace the manual stamping of passports with individual files in a centralised database, which will be operated by eu-Lisa. The aim is to identify individuals who stay longer within the Schengen area than permitted, referred to in the legislation as "overstayers".[170] The system will also be used to facilitate the automation of border controls, through the storage of biometric data and the use of 'e-gates' at border crossings – although the feasibility of using such technology at all border crossing points remains to be seen.[171] Data held in the EES will also be available to law enforcement authorities under certain conditions. The legislation was finalised in November 2017.

Each individual file will contain biographic and biometric data in individual records detailing the time, place and date of each entry into and departure from the Schengen area.[172] Files will also be stored on individuals refused entry.[173] The biographical data held in the system will include name, date of birth and nationality, information on travel documents, a facial image (from both visa-obliged and visa-exempt travellers) and four fingerprints (from visa exempt-travellers).[174] Visa-obliged travellers will already have a scan of ten fingerprints stored in the central database of the Visa Information System (VIS), which will be made accessible to officials via interconnection with the EES. The files in the EES will be retained for three years after the last recorded exit of an individual but, if no exit is recorded, the data will be held for five years. The data stored in all files will be made available to Frontex for carrying out "risk analyses and vulnerability assessments".[175]

To identify and detect people who have overstayed their visa, all border-crossings of individuals covered by the system will be logged in a centralised database and used to update an "automated calculator". This will tell officials at the border and in-country how much longer an individual may remain in the Schengen area (or how long they have overstayed for).[176] The system will also automatically generate and transmit lists of people who have overstayed their visa to the relevant national authorities, so that they can "adopt appropriate measures."[177] Those measures must be in accordance with national, rather than EU, law. If an individual is found to have overstayed when they are checked against the central database whilst exiting the Schengen area, for example, they may be subjected to a fine or other sanction. On the other hand, if they are subject to an identity check in the street and found to be in the Schengen area without the requisite permission, they could be subjected to detention and deportation.

170 The precise definition of "overstayer" is "a third-country national who does not fulfil or no longer fulfils the conditions relating to the duration of his or her authorised short stay on the territory of the Member States". Article 3(19), Regulation (EU) 2017/2226

171 eu-LISA, 'Working Group on ICT Solutions for External Borders (sea/land) Report', 26 March 2019, https://www.eulisa.europa.eu/Publications/Reports/WG%20on%20ICT%20Solutions%20for%20External%20Borders%20-%20Report.pdf

172 'Chapter II – Entry and use of data by competent authorities', Regulation (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226#d1e2007-20-1

173 Article 18, Regulation (EU) 2017/2226

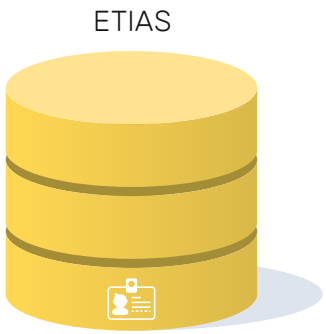
174 Articles 15-20, Regulation (EU) 2017/2226

175 Article 63(1), Regulation (EU) 2017/2226

176 Article 11(2)(a)-(d), Regulation (EU) 2017/2226

177 Article 12, Regulation (EU) 2017/2226

5. European Travel Information and Authorisation System (ETIAS)



The ETIAS applies to persons who do not require a visa to enter the Schengen area. It will be used to examine whether individuals are a "security, migration or health" risk by comparing travel authorisation applications to EU databases and information systems, Europol data and Interpol data. It will also make use of a 'watchlist' and an automated profiling system, through which data from an individual's application form will be compared to a series of 'risk indicators'. Similar systems operate elsewhere in the world, for example in Australia (Electronic Travel Authority), Canada (Electronic Travel Authorization) and the USA (Electronic System for Travel Authorization).

While the ETIAS has a broadly similar structure to the other large-scale information systems examined here (a central system connected to an interface in each Member State), it differs from those systems in that biometric data is not processed in the ETIAS. Biographic data captured by the system will include items such as names, place and date of birth, and travel document information. Applications will also require, amongst other things: parents' first names; home address, email address, education, occupation and the Member State of first intended stay.[178] Applicants must also provide answers to questions on:

- whether they have been convicted of certain criminal offences[179] over the previous 10 years (20 years in the case of terrorist offences) and where;
- whether they have "stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay"; and
- whether they have been expelled from any of the Member States, any of the countries on the EU's 'visa list', or have been subject to any return decision in the previous 10 years.[180]

An affirmative answer to any of these questions will require the provision of answers to "an additional set of predetermined questions on the application form by selecting from a predetermined list of answers"[181] (the specific content and format of both sets of questions will be determined in delegated acts to be adopted by the Commission[182]). Completed and paid-for applications (the process will cost €7[183]) will then be transmitted to the ETIAS Central System where certain data items[184] will be

178 Article 17(2), Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

179 The list contained in the Annex to the Regulation is essentially the same as the list of crimes covered by the European Arrest Warrant (EAW), with the exclusion of swindling and the addition of industrial espionage. However, unlike the minimum sentencing requirements that give rise to surrender pursuant to a EAW (punishable in the EAW-issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years), the ETIAS rules do not require any minimum sentencing length or other threshold to require inclusion in the application form.

180 Article 17(4), Regulation (EU) 2018/1240

181 Article 17(6), Regulation (EU) 2018/1240

182 Articles 17(5) and (6), Regulation (EU) 2018/1240

183 Article 18(1), Regulation (EU) 2018/1240

184 Article 20(2), Regulation (EU) 2018/1240

automatically compared against other EU and non-EU databases and information systems.[185] This process will determine, for example, whether the applicant: is using a travel document reported as lost or stolen; is subject to a refusal of entry and stay alert entered in SIS; has ever been reported as a personal who has overstayed their visa in the EES; or has been registered in Eurodac.[186]

Certain data items will also be compared to the 'ETIAS watchlist' (compiled by the Member States and Europol and listing persons suspected of involvement, either in the past or future, in terrorist or other serious criminal offences[187]) and to the 'ETIAS screening rules' (an "algorithm enabling profiling" allowing data from applications to be compared with "specific risk indicators"[188]). The factors that will form the basis for the specific risk indicators will be set out in an implementing act to be adopted by the Commission and reviewed at least every six months,[189] while the indicators themselves will be "defined, established, assessed ex ante, implemented, evaluated ex post, revised and deleted by the ETIAS Central Unit, after consultation of the ETIAS Screening Board."[190] The Screening Board will be made up of representatives of Frontex, Europol and each Member State's ETIAS National Unit,[191] and when issuing recommendations (for example in relation to the risk indicators) must "take into consideration the recommendations issued by the ETIAS Fundamental Rights Guidance Board," which has an "advisory and appraisal function," but no binding powers.[192]

Where any of this automated processing results in one or more hits, the application will be referred to the ETIAS Central Unit for further examination.[193] If the hits were 'false', the Central Unit approves the application; otherwise, it must be passed to the relevant ETIAS National Unit for a more detailed assessment and the subsequent approval or denial of the application.[194] Successful applicants will then be able to travel to the Schengen area (although they may still be denied entry) and their entries and exits will duly be logged in the EES. Travel authorisations will be valid for three years or until the end of the validity of the travel document used in the application;[195] this period may be extended for a further three years with the consent of the applicant.[196] Refused applications will be stored for five years.[197]

185 Article 20(2): "the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol SLTD and TDAWN databases."

186 Article 20(a), (b), (c) and (g), Regulation (EU) 2018/1240

187 Article 34(1) and (3), Regulation (EU) 2018/1240

188 Article 33(1), Regulation (EU) 2018/1240

189 Article 33(3), Regulation (EU) 2018/1240

190 Article 33(6), Regulation (EU) 2018/1240

191 Article 9(1), Regulation (EU) 2018/1240

192 Article 9(3). The Fundamental Rights Guidance Board will be made up of Frontex's Fundamental Rights Officer and representatives of: the Frontex Consultative Forum on Fundamental Rights, the European Data Protection Supervisor, the European Data Protection Board and the Fundamental Rights Agency (Article 10(1).

193 Article 22(5), Regulation (EU) 2018/1240

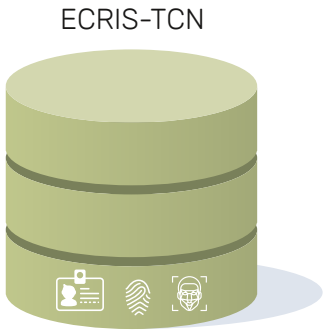
194 Article 26, Regulation (EU) 2018/1240

195 Article 36(5), Regulation (EU) 2018/1240

196 Article 54(2), Regulation (EU) 2018/1240

197 Article 54(1)(b), Regulation (EU) 2018/1240

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



The ECRIS-TCN is designed to make it easier for the authorities of one Member State to obtain the criminal records of non-EU nationals convicted in another Member State. As with the other systems examined here, the ECRIS-TCN will consist of a centralised database managed by eu-Lisa, with connections to a central access point in each Member State. A key justification for the establishment of a centralised database containing biometric identifiers was its usefulness for the interoperability initiative.[198] The central database will hold identity data (biographic data, fingerprints and in certain cases facial images). If a search in the ECRIS-TCN returns a "hit", the searching authority will use the existing ECRIS network to request further information.

Legislation establishing the original ECRIS was approved in 2009[199] and the system began functioning in 2012. It is used for transferring information extracted from national criminal records between EU Member States. That information can be used in criminal proceedings (in which case provision of the information is mandatory) or for "purposes other than criminal proceedings" (in which case information can only be provided if it is permitted by the national law of the two Member States involved in the transaction). The system was introduced to help implement the obligation for convictions handed down in other Member States to be taken into account in criminal proceedings.[200]

According to the legislation establishing ECRIS, every Member State must ensure that all its criminal records include information on the nationality or nationalities of the convicted person. When one or more of those nationalities is that of another Member State, that other Member State (the "Member State of nationality") must be informed of and store information on convictions. Information on any subsequent alterations or deletions to the information in the criminal record must also be sent to the Member State of nationality, so that it becomes the central repository for their criminal record. However, because non-EU states do not participate in the ECRIS, information on the criminal records of non-EU nationals is not systematically available to Member States unless 'blanket requests' are made to all other Member States, in order to see whether they hold such information. As the agreed text of the ECRIS-TCN Regulation says, this puts "a disproportionate administrative burden on all Member States, including those not holding information on the third-country national."[201] In order to ensure maximum 'coverage', dual nationals holding an EU passport and a non-EU

198 The proposal argued that "interoperability would not be possible if a decentralised solution as proposed in January 2016 would have been pursued." See: SWD(2016) 04 final, 19 January 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

199 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009F0315; Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0316

200 This obligation was introduced by a Council Framework Decision in 2008: Council Framework Decision of 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0675

201 Recital 6, Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0816

passport will also be included in the system, a decision which drew sharp criticism.[202]
The files stored in the central database will include a set of biographic data[203] and at least one (but possibly two) biometric identifiers. The inclusion of fingerprints in the system will be mandatory and based on two criteria. The first of these is existing national law, where it deals with such matters. If it does not, fingerprints must be captured and stored from any non-EU national convicted "to a custodial sentence of a minimum of six months" or convicted of an offence punishable under national law "by a custodial sentence for a maximum period of at least 12 months." This new criteria will, in many Member States, introduce a new requirement for fingerprinting convicted non-EU nationals, provided that their conviction meets one of the two thresholds, even though there may be no such requirement for EU nationals.[204]

Facial images will be added to the files in the central database "if the law of the convicting Member State allows for the collection and storage of facial images of convicted persons."[205] This will make it possible to retrieve facial images from the database, but it will only be possible to use them as a search key if an assessment to be conducted by the Commission gives the green light to do so.[206] A Directive on ECRIS-TCN, which accompanies the Regulation and also amends aspects of the existing ECRIS, will introduce a requirement for national authorities to provide facial images of EU nationals as part of their response to requests for information through the existing ECRIS, if they are available to the central authority.[207]

Member States' authorities will be able to use the system to request information for use in both criminal and non-criminal proceedings. Regarding the latter, the agreed text sets out seven possible non-criminal proceedings for which requests can be made,[208] although Member States can also decide upon their own purposes, "if provided under and in accordance with national law." In this case, they will have to notify the European Commission of these other purposes so that they can be published in the Official Journal of the EU. Three EU agencies will also be able to access the system, for various reasons: Europol, Eurojust and the European Public Prosecutor's Office (EPPO).[209]

202 Letter from the Meijers Committee to Claude Moraes MEP, 'The fundamental right to non-discrimination', 22 January 2019, https://www.commissie-meijers.nl/sites/all/files/cm1902_ecris-tcn_and_the_fundamental_right_to_non-discrimination_0.pdf

203 According to Article 5(1)(a)(i), the following alphanumeric data will be obligatory: surname (family name); first name(s) (given names); date of birth; place of birth (town and country); nationality or nationalities; gender; previous name(s), if applicable; the code of the convicting Member State. Parents' names may also be included, if they are contained in the national criminal record, and if it is available to the national central authority then the following should also be included: identity number, or the type and number of the person's identification document(s), as well as the name of the issuing authority thereof; pseudonym and/or alias name(s).

204 In a document accompanying the January 2016 proposal for a Directive, the Commission noted that "a number of Member States have expressed constitutional concerns… Many Member States do currently not use fingerprints in their national criminal record registers," and that "some Member States are concerned about possible double standards for EU nationals on the one hand and TCN [third-country nationals] on the other hand… not all convicted persons contained in the national criminal record registries have had fingerprints taken, as national rules differ according to categories offences and between Member States." See: Footnote 32, p.15, SWD(2016) 4 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

205 Article 5, Regulation (EU) 2019/816

206 Article 6(2), Regulation (EU) 2019/816

207 Contained in a new Article 11(1)(c)(iv) to be added to Framework Decision 2009/315/JHA, as amended by Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 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, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019L0884

208 Article 7(1): Checking person's own criminal record at their request; security clearances; obtaining a license or permit; employment vetting; vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons; visa, acquisition of citizenship and migration procedures, including asylum procedures; and checks in relation with public contracts and public examinations.

209 Article 14 of the Regulation; see also the annex to: 'Disproportionate and discriminatory: the European Criminal Records Information System on Third-Country Nationals (ECRIS-TCN), February 2019, http://www.statewatch.org/analyses/no-340-ecris-tcn.pdf

design: chocolatejesus.be

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

Rue du Congres / Congresstraat 37-41, post box 5
1000 Brussels
Belgium
Tel: +32/2/210 17 80
Fax: +32/2/210 17 89
info@picum.org
www.picum.org