Funded by
the European Union

EMN
European Migration Network

Processing the biometric data of third-country nationals

European Migration Network Inform

December 2024

Disclaimer

The European Migration Network (EMN) is a Europe-wide network providing information on migration and asylum. The EMN consists of National Contact Points (NCPs) in the EMN Member (EU Member States except Denmark) and Observer Countries (NO, GE, MD, UA, ME, AM, RS, MK), the European Commission and is supported by the EMN Service Provider. The inform does not necessarily reflect the opinions and views of the European Commission, the EMN Service Provider (ICF) or the EMN NCPs, nor are they bound by its conclusions. Similarly, the European Commission, the EMN Service Provider (ICF) and the EMN NCPs are in no way responsible for any use made of the information provided.

Explanatory note

This inform was prepared on the basis of national contributions from 27 EMN NCPs (AT, BE, BG, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, PT, SE, SI, SK, and NO, UA, RS) collected via an AHQ developed by the EMN NCPs to ensure, to the extent possible, comparability. The information contained in this inform refers to the situation in the abovementioned EMN Member and Observer Countries up to March 2024.

Published

December 2024

Suggested citation

European Migration Network (EMN), 'Processing of biometric data of third-country nationals - EMN inform', [Date], [URL], last accessed on [day month year].

For more information

EMN website: http://ec.europa.eu/emn
EMN LinkedIn page: https://www.linkedin.com/company/european-migration-network
EMN X account: https://twitter.com/emnmigration
EMN YouTube page: https://www.youtube.com/@EMNMigration

Icons made by Freepik from www.flaticon.com and vecteezy.com. Cover image: iStockphoto

CONTENTS

1. KEY POINTS TO NOTE 4

2. INTRODUCTION 4
   Main aim and scope of the inform 4

3. DEFINITIONS 5

4. COLLECTION OF BIOMETRIC DATA 6
   Migration processes in which biometric data is collected 7
   Specific biometric identifiers collected 8
   Specific rules for collecting and processing biometric data based on age or to ensure non-discrimination 9
   Initial purpose for collecting Biometric data 9

5. STORAGE OF BIOMETRIC DATA 10
   Data controller for the collection and processing of biometric data under national legislation 10

6. PROCESSING OF BIOMETRIC DATA FOR A PURPOSE OTHER THAN THE INITIAL PURPOSE 10
   Processing of biometric data for law enforcement, national security or other purposes 10
   Processing of biometric data for SIS alerts 11

7. INTERNATIONAL TRANSFER OF BIOMETRIC DATA 12

1. KEY POINTS TO NOTE

This inform gathers information on current national legislation and practices for the collection and processing of biometric data of third-country nationals in 24 European Migration Network (EMN) Member Countries and foreign migrants in three Observer Countries,[1] in accordance with European Union (EU) law, treaties of the Council of Europe, or national law.

For each of the specific migration processes examined, the majority of EMN Member and Observer Countries collect and process biometric data to at least some extent.

- Biometric data are most commonly collected from individuals applying for international protection, individuals applying for a long-stay visa or a residence permit, and individuals applying for a short-term visa. Biometric data are collected less often during the return or removal process, or during the border crossing process.
- Eighteen countries cite a separate national legal framework for collecting biometric data during the international protection process, while nine specify separate national legislation for collecting biometric data during the short-term visa process.
- Biometric facial images and fingerprints are the most common types of biometric data and are collected by all countries across all relevant processes.
- All 27 responding EMN Member and Observer Countries have specific rules or practices for biometric data collection based on the age of the person concerned. These rules commonly include an age limit under which fingerprints cannot be collected, varying from 6, 12, and 14 years of age, depending on the country and the specific migration process. Some countries apply a general age limit and others specify different limits for different migration processes.
- Many EMN Member Countries include specific rules to ensure non-discrimination. These rules include practical accommodations during biometric data collection for people with physical disabilities or specific religious/cultural needs, as well as rules for storage and processing of specific categories of data, such as data identifying religious or political affiliation.
- The initial purpose of collecting biometric data was primarily for the identification of an individual, the verification of an individual's identity, or of the authenticity of travel documents. Five countries also specified that national security, criminal investigation, or law enforcement served as an initial purpose for the collection of biometric data during migration processes.
- All but one country stated that they stored biometric data in a national repository during at least one of the relevant migration processes. The rules for data storage across the EMN Member and Observer Countries vary widely.
- A majority of countries allow processing of biometric data stored in national repositories for the purposes of Schengen Information System (SIS) alerts,[2] although many do not allow use of these data for all categories of SIS alerts.[3] Fourteen countries allow biometric data to be used for alerts on return under Regulation (EU) 2018/1860[4] and alerts for refusal of entry and stay under Regulation (EU) 2018/1861.[5]
- The majority of countries allow the processing of biometric data for other purposes, including security and criminal investigations.
- Twenty-one countries allow international transfer of biometric data,[6] typically limited to specific uses or situations. Twelve report international transfer of data is allowed where it is explicitly allowed or required by law, a specific international legal obligation such as a treaty or EU regulation.[7] Six countries also allow sharing of data with third countries to facilitate the return or removal process.[8]

2. INTRODUCTION

Main aim and scope of the inform

This inform examines current national legislation and practices for the collection and processing of biometric data of third-country nationals in 24 EMN Member Countries and of foreign migrants in three Observer Countries,[9] in accordance with the requirements of national and European law (EU law and the treaties of the Council of Europe).

It addresses the legal framework on data protection, including the General Data Protection Regulation (GDPR) (2016/679/EU),[10] the Data Protection Law Enforcement

1 AT, BE, BG, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, PT, SE, SI, SK and NO, UA, RS.
2 Regulation 2018/1860 and Regulation 2018/1861 do not apply to Ireland.
3 Only six countries allow processing of these data for all types of alerts considered: CZ, DE, EE, ES, HU and NO.
4 AT, BE, CZ, DE, EE, ES, HR, HU, LT, NL, PL, SE, SK and NO.
5 AT, BE, CZ, DE, EE, ES, HU, IT, LT, NL, PL, SE, SK and NO.
6 AT, BE, BG, DE, ES, FI, FR, HR, HU, IE, IT, LT, LV, NL, PL, SE, SI, SK and NO, UA, RS.
7 AT, DE, ES, FI, HU, IE, IT, LV, LT, PL, SE and NO, RS.
8 BE, FI, HR, IE, NL and RS.
9 NO, UA, and RS.
10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://data.europa.eu/eli/reg/2016/679/oj, last accessed on 10 December 2024.

Directive (LED) (2016/680/EU),[11] and the Regulations[12] on large-scale information technology (IT) systems for freedom, security and justice.[13] It also addresses the applicable legal framework on fundamental rights, including the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,[14] European Court of Human Rights (ECtHR) case-law on biometric data,[15] and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).[16]

The inform focuses on the collection and processing of biometric data in all areas of migration management.

Data collection revealed that data collected in migration processes were in some cases also used for a secondary purpose in relation to law enforcement (see Section 6). Biometric data is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.[17] The inform covers the collection of biometric data in migration process, the initial purpose of collecting those data, storage, processing for purposes other than the initial purpose, and international transfer of biometric data.

3. DEFINITIONS

The inform uses the following definitions, which are based on the EMN Asylum and Migration Glossary, unless otherwise stated.[18]

Term	Definition
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique **identification** of that natural person, such as facial images or dactyloscopic data
Child	Every human being below the age of 18 years, unless, under the law applicable to the child, majority is attained earlier or later
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.[19]

11 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, http://data.europa.eu/eli/dir/2016/680/oj, last accessed on 10 December 2024.

12 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), http://data.europa.eu/eli/reg/2008/767/oj as amended by http://data.europa.eu/eli/reg/2021/1134/oj, last accessed on 10 December 2024; Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, http://data.europa.eu/eli/reg/2017/2226/oj, last accessed on 10 December 2024; 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) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, http://data.europa.eu/eli/reg/2018/1240/oj, last accessed on 10 December 2024; 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) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, http://data.europa.eu/eli/reg/2019/816/oj, last accessed on 10 December 2024; 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 (Schengen information system (SIS)) http://data.europa.eu/eli/reg/2018/1860/oj, last accessed on 10 December 2024; 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, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, http://data.europa.eu/eli/reg/2018/1861/oj, last accessed on 10 December 2024; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU http://data.europa.eu/eli/reg/2018/1862/oj, last accessed on 10 December 2024; Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) (Eurodac Regulation), http://data.europa.eu/eli/reg/2013/603/oj, last accessed on 10 December 2024; 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 and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, http://data.europa.eu/eli/reg/2019/817/oj, last accessed on 10 December 2024; 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 and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, http://data.europa.eu/eli/reg/2019/818/oj, last accessed on 10 December 2024.

13 Council of Europe, 'IT systems to fight crime and secure EU borders', n.d., https://www.consilium.europa.eu/en/policies/it-systems-security-justice/, last accessed on 19 July 2024.

14 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005, last accessed on 10 December 2024.

15 Case of S. and Marper v. the United Kingdom [GC], no 30562/04 and 30566/04, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}, last accessed on 10 December 2024.

16 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108, last accessed on 10 December 2024. The Convention does not cover biometric data, but the draft explanatory report of the modernised version of Convention 108 (T-PD-BUR(2013)3ENrev5) referred to biometric data, https://rm.coe.int/bureau-of-the-consultative-committee-of-the-convention-for-the-protect/168073dc56, last accessed on 10 December 2024. The Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) would extend the protection to biometric data once ratification conditions are met, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223, last accessed on 10 December 2024.

17 GDPR, Article 4(14).

18 EMN Glossary, https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_en, last accessed on 4 December 2024.

19 GDPR, Article 4(7).

Term	Definition
Country of return	In the EU context, a third country to which a third-country national returns
Establishment of identity	Process which is commonly carried out for identification and identity-verification purposes in different procedures on the basis of a review of documentary evidence, but which makes use of different procedures and methods when documentary evidence may be inauthentic, inadequate, insufficient or absent
Eurodac	An information system, the purpose of which, via the collection, transmission and comparison of fingerprints, is to assist in determining which EU Member State is to be responsible pursuant to Regulation (EU) No 604/2013 (Dublin III Regulation) for examining an application for international protection lodged in a EU Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No 604/2013 under the conditions set out in the Regulation establishing Eurodac
Identification	The process of determining a person's identity through a database search against multiple sets of data (one-to-many check)
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[20]
Removal	In the *global context*, the act of a state in the exercise of its sovereignty in removing an alien from its territory to a certain place after refusal of admission or termination of permission to remain. In the *EU context*, the enforcement of the obligation to return, namely the physical transportation out of the EU Member State
Schengen Information System (SIS)	An information exchange system for security, migration and border management, with the aim of ensuring a high level of security within the EU and the Schengen Associated Countries by supporting operational cooperation between competent national authorities, in particular border guards, the police, customs authorities, immigration authorities, and authorities responsible for the prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties and ensuring that the movement of persons is in conformity with EU rules[21]
Temporary protection	A procedure of exceptional character to provide, in the event of a mass influx or imminent mass influx of displaced persons from third countries who are unable to return to their country of origin, immediate and temporary protection to such persons, in particular if there is also a risk that the asylum system will be unable to process this influx without adverse effects for its efficient operation, in the interests of the persons and other persons requesting protection
Third country	A country that is not a member of the European Union as well as a country or territory whose citizens do not enjoy the European Union right to free movement, as defined in Article 2(5) of Regulation (EU) 2016/399 (Schengen Borders Code)
Third-country national	Any person who is not a citizen of the European Union within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union (TFEU) and who is not a person enjoying the European Union right to free movement, as defined in Article 2(5) of Regulation (EU) 2016/399 (Schengen Borders Code)
Verification of identity	The process of comparing sets of data to establish the validity of a claimed identity of a person (one-to-one check)
Visa Information System (VIS)	A system for the exchange of visa data between EU Member States, which enables authorised national authorities to enter and update visa data and to consult this data electronically

4. COLLECTION OF BIOMETRIC DATA

This inform examines biometric data collection practices across six categories of migration processes. The processes include applying for international protection, applying for a residence permit or long-stay visa, applying for a short-term visa, the return or removal process, the border crossing process, and other miscellaneous processes such as applying for temporary protection, issuing travel documents for non-citizens (e.g. aliens' passports), or citizenship. For each of these processes, EMN Member and Observer Countries specify whether they collect biometric data, specific biometric identifiers collected, whether national legislation contains specific rules on age, whether national legislation contains specific rules to ensure

20 GDPR, Article 4(2).
21 Derived by EMN from recital 1 and Article 1 of Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and recital 1 and Article 1 of Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters.

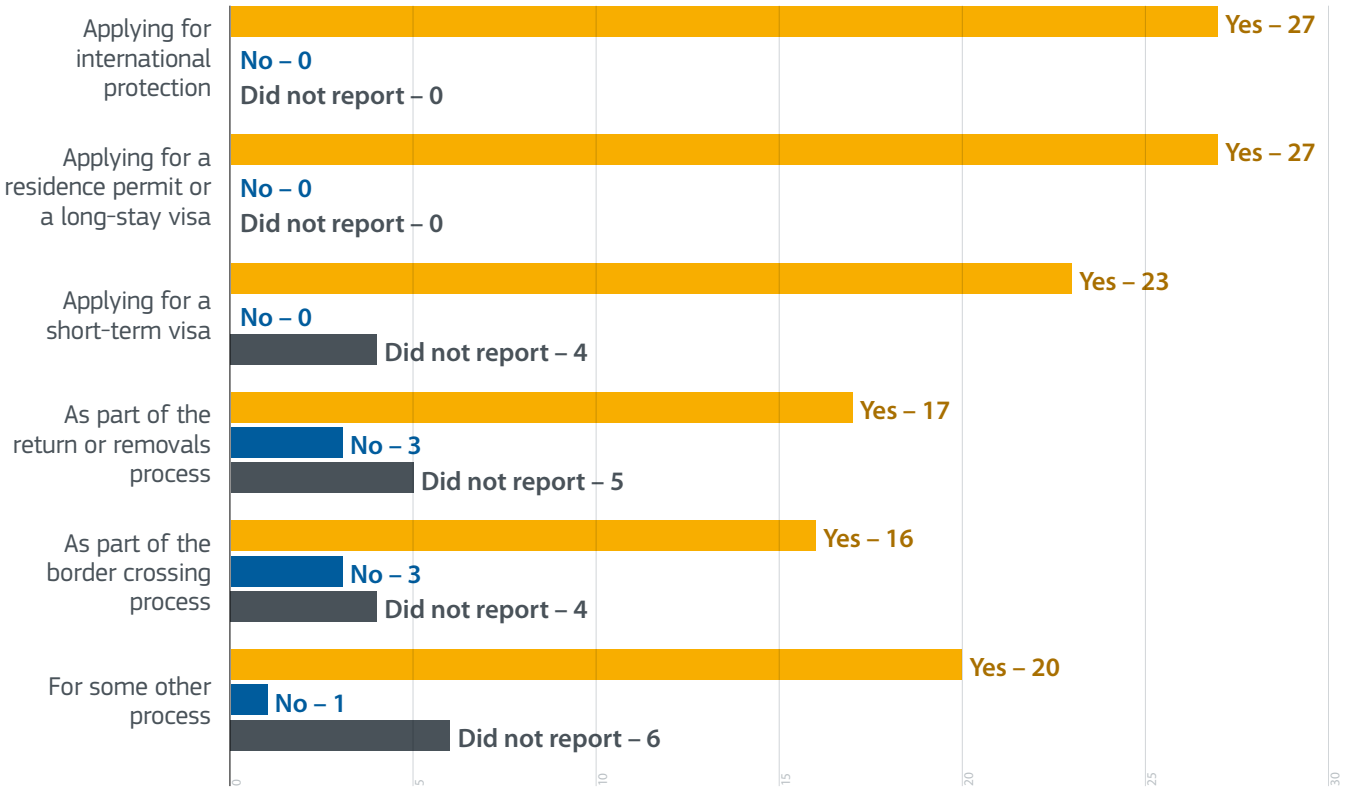
non-discrimination, and the initial purpose(s) of collecting biometric data.

Migration processes in which biometric data is collected

National legislation and practices vary widely between EMN Member and Observer Countries in respect of the specific migration process and circumstances for which they collect biometric data. At least 16 of the 27 responding countries collect biometric data to some degree under each of the specific migration processes examined (see Figure 1). Biometric data are most commonly collected from individuals applying for international protection, applying for a long-stay visa or a residence permit, and applying for a short-term visa. Biometric data are least commonly collected during the return or removal process, or during the border crossing process.

Figure 1 provides an overview of biometric data collection by these specific categories of migration process as reported by EMN Member and Observer Countries.

Figure 1: Biometric data collection, by migration process



Source: EMN Member and Observer Countries

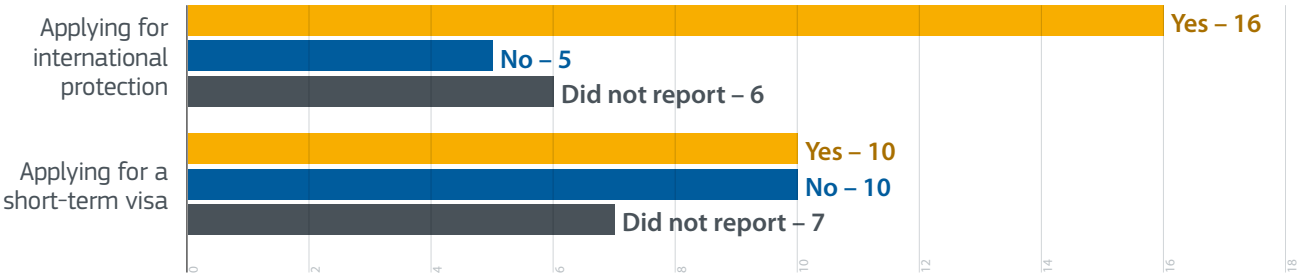
All EMN Member and Observer Countries confirm that they collect biometric data for individuals applying for residence or a long-stay visa and for individuals applying for international protection. For EU Member States and Norway, the Eurodac Regulation directly provides for collection of biometric data during the international protection process.

Nineteen EMN Member and Observer Countries cite a national legal framework covering collection of biometric data of individuals applying for international protection.[22]

Figure 2 shows the extent to which there is national legislation on the collection of biometric data.

22 AT, BE, BG, EE, ES, FI, FR, HR, IE, LT, LU, LV, NL, PL, SI, SK and NO, RS, UA.

Figure 2: National legislation on the collection of biometric data



Source: EMN Member and Observer Countries

Of the 27 responding EMN Member and Observer Countries, 24 also indicated that they collect biometric data for short-term visas.[23] EU law requires collection of these data under the VIS Regulation and many countries collect this data based on EU law without complementary national legislation. Two EMN Member and Observer countries did not specify whether they collect these data.[24] In Cyprus, data will be collected from 2025, following technical updates to the system. Of the 24 countries reporting that they collect these data, 10 do so under the VIS Regulation without separate national legislation,[25] 10 have national legislation on the collection of biometric data for short-term visas,[26] and three did not specify.[27] In Sweden, some forms of biometric data, including photographs, are collected under the VIS Regulation but stored under national legislation. Fingerprints are collected but not stored nationally in Sweden.

Eighteen EMN Member and Observer Countries collect biometric data as part of the return or removal process,[28] 16 as part of the border crossing process,[29] and 21 as part of some other process, primarily the issuance of travel documents such as refugee passports, passports for foreigners, or other identification documents.[30] Other processes include applications for citizenship,[31] temporary protection,[32] or in relation to irregular crossing or irregular stay.[33]

Specific biometric identifiers collected

Photographs, facial images and fingerprints are the most common forms of biometric data collected among EMN Member and Observer Countries across all migration processes, with all countries collecting one of these forms of biometric data during the relevant migration processes. Thirteen countries record a different quantity of data depending on the process. This difference may derive from different requirements under EU law. For example, Latvia collects a facial image and at least two fingerprints in most processes. The Visa Code (Regulation (EU) 810/2009)[34] requires the collection of 10 fingerprints when applying for a short-term visa and Latvia applies this requirement. Similarly, Slovenia collects two fingerprints for residence applications and 10 fingerprints for a short-term visa, as per the Visa Code.

Six countries reported that, under some circumstances, DNA samples could be taken.[35] Collection of DNA samples is typically limited to specific situations. Norway can take DNA samples where there is a need to confirm the family relationship of an individual. In Slovenia, DNA evidence can be collected only under the return and removal and border control processes where the identity of the individual cannot otherwise be established. The Netherlands can collect DNA samples to send to the Dutch Forensic Institute to confirm family relationships who performs the DNA investigation and provides the results to the Immigration Service. The DNA sample collected for this purpose is destroyed after six months. Finally, Italy conducts DNA examinations during the family reunification process only when documentation proving the family relationship is missing or has formal irregularities.

Eight countries can take additional personal data along with biometric data, such as a signature.[36] In Finland, in some processes, other information may also be collected, including hair and eye colour, weight, and handedness (dominant hand of an individual).

23 AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, SE, SI, SK and NO, RS. Ireland is not bound by the visa code and collects biometric data for short stay visas under national law. Fingerprints are collected from applicants resident in China (including Hong Kong), India, Nigeria and Pakistan.
24 PT and UA.
25 CZ, ES, FI, HR, HU, IT, NL, PL, SE, SI, SK.
26 BG, DE, EE, FR, IE, LT, LU, LV, PL and NO, RS.
27 AT, BE, EL.
28 AT, BE, CZ, DE, EE, ES, FI, FR, HR, IE, HU, LT, LU, LV, PL, SK and UA, RS. Norway's national law provides for collection of biometric data, but these data are not collected in practice.
29 BE, BG, CZ, DE, EE, FI, FR, HR, IE, LU, LV, PL, SI, SK and UA, RS. In Belgium, data are taken for short-term visa holders at this time only to match with data in the VIS system and are not stored. Lithuania does not collect data during this process, but matches biometric identifiers against existing data. In Ireland, border officials may take fingerprints from visa-required persons from whom fingerprints were collected as part of the visa application process, as a verification check at the border.
30 AT, CY, DE, EE, ES, FI, FR, LT, LU, LV, NL, PT, SE, SI, SK and NO, UA.
31 EE, EL, ES, FR, LT.
32 EE, EL, FI, HU, LV, SI, SK. In Ireland, biometric data are not collected as part of the temporary protection registration process. However, beneficiaries of temporary protection also register their residence permission under the Immigration Act 2004 and biometric data are collected as part of that registration process, as per all registration applications. The registration process does not confer any additional entitlements on beneficiaries of temporary protection.
33 ES, LV, NL, PL and NO.
34 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), last accessed on 4 November 2024.
35 BG, EE (not done in practice), IT, NL, SI and NO.
36 AT, CY, EE, FI, LT, NL, PT and UA.

Specific rules for collecting and processing biometric data based on age or to ensure non-discrimination

All EMN Member and Observer Countries have specific rules or practices for collecting and processing data depending on the age of the person concerned. These specific rules or practices consist primarily of age limits for the collection of biometric data. Biometric data must be collected and transferred to Eurodac for individuals of at least 14 years of age to establish the identity of applicants for international protection and persons apprehended in connection with the unlawful crossing of the external borders of the Union, as well as to allow each Member State to check whether a third-country national or stateless person found illegally staying on its territory has applied for international protection in another Member State. For national purposes, the biometric data of children younger than 14 may also be collected, but not included in Eurodac.[37] Fingerprints must be taken from children from the age of 12 according to the Visa Code requirements,[38] and from the age of six for residence permits.[39]

Ten countries reported they do not go beyond current Eurodac requirements to collect fingerprint data during applications for international protection for applicants under the age of 14.[40] Fourteen countries do not collect biometric data from children under the age of six for long-stay visas and/or residence permits.[41]

Fourteen countries specify different age limits for different processes.[42] Sweden has a minimum age of 14 for collecting data for applications for international protection, but a minimum age of six for residence permits, short and long-stay visa applications, and other processes such as alien passports and travel documents. In Ireland, fingerprints are not taken for visa applications from children under the age of five. In general, children under 16 are not required to register for immigration permission in Ireland, thus no data are collected. Eight countries reported general requirements for age:[43] in Hungary, biometric data in general is not taken below the age of 14; in Serbia, fingerprints are not collected from minors under the age of 12. These age limits may apply only to fingerprints. The Netherlands, Norway and Greece all report that a facial image is collected regardless of age.

Seven countries[44] have additional protections in place when collecting or processing the biometric data of minors, such as child-friendly treatment in Germany, Poland and Spain.

Only two EMN Member Countries specified an upper age limit for biometric data collection.[45] In Estonia, people over the age of 70 are not fingerprinted when applying for permanent residence or a long-term residence permit, or when preparing an identity card or long-term residence permit card, as long as their fingerprints were previously collected and entered into the automatic biometric identification system database. Poland has an upper age limit of 100 years old for processing and storing biometric data by the police.

Thirteen EMN Member and Observer Countries have specific rules in their national legislation or practice on the collection and processing of biometric data of specific groups to ensure non-discrimination.[46] These include adapted requirements for the fingerprinting process to accommodate people who, for medical reasons, are unable to provide fingerprints at all or are unable to provide the full range of fingerprints normally required.[47] Three countries also outline specific requirements for collecting, storing and sharing data that may reveal characteristics such as racial or ethnic origin, religious belief, or in a way that may result in discrimination.[48] Five countries have adapted biometric data collection to account for religious, cultural, or physical needs, such as photograph requirements allowing religious headwear or wearing dark glasses for individuals with visual impairments, or accommodating requests for biometric data to be collected by a person of the same sex.[49]

Initial purpose for collecting Biometric data

The most common initial purpose for collecting biometric data identified by EMN Member and Observer Countries across the migration processes examined is to establish and verify the individual's identity. The most common uses of these data include verifying the identity of a person or the authenticity of a travel document,[50] or for the administrative process of issuing identification documents.[51]

National security, security, criminal investigation or law enforcement can, under some circumstances, be an initial purpose for collecting biometric data in migration processes. Five EMN Member Countries specifically identify national security, security, law enforcement, or investigation as initial purposes for collecting biometric data in different migration processes.[52] In Croatia, security is included in law as an initial purpose for collecting biometric data for the short-term visa process, the detection and investigation of criminal offences are included in law as initial purposes for

37 Currently beyond the requirements of Eurodac, although this will change with the revised Eurodac Regulation in force from 2026, when biometric data will be collected from children from the age of six (Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council, last accessed on 10 November 2024.
38 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), last accessed on 4 November 2024.
39 Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, last accessed on 10 November 2024.
40 AT, BE, CY, CZ, EE, EL, FR, HR, IE, LT, LU, LV, SE and RS.
41 AT, BE, CY, DE, EE, EL, FI, HR, LT, LV, PL, SE, SI, SK.
42 AT, BE, CY, EE, EL, HR, LT, LV, PL, SE, SI, SK and NO, RS.
43 ES, FR, IT, LU, NL, PT and UA, RS.
44 DE, EE, ES, FI, HR, PL and RS.
45 EE, PL.
46 BG, CY, EE, EL, FR, HR, IT, LT, LU, PL, SI and UA, RS.
47 CY, DE, EL, ES, HR, IT, LT, LU, NL, PL.
48 BG and RS.
49 CY, DE, LT, NL, PL and RS.
50 AT, CZ, EE, EL, FI, FR, HR, IE LT, LV, NL, SI, SK, and NO, UA.
51 CY, EE, ES, FI, IE, IT, LT, LV, NL, PL, and NO, RS.
52 BE, CZ, EL, HR, FI.

the collection of biometric data for the removal and return process, and investigation and prevention of crime are included for the border control process. Finland cites national security as an initial purpose for collecting biometric data in most migration processes, and Greece cites national security as an initial purpose for biometric data collection under the short-term visa process.

5. STORAGE OF BIOMETRIC DATA

Storage processes vary considerably. For example, Spain's national law does not contain a uniform rule. In Ukraine, data are generally stored no longer than necessary to undertake the purpose for which those data were stored. In Norway, the storage time for biometric data under national legislation is very complex and varies significantly, depending on the type of case for which the data are stored. For this reason, Norway may soon revise its legislation.

All but one EMN Member and Observer Country store biometric data in a national repository in at least some form or during at least one of the migration processes. Only France does not store biometric data in a national repository, but, rather, stores the data collected for each of the relevant migration processes in a dedicated, automated process, depending on the relevant procedure and retains the data for only a limited period, in accordance with national rules.[53]

The length of time for which the data are stored varies by country and by migration process. Many countries did not specify the storage time applicable to the different migration processes. The Slovak Republic allows data to be stored during the international protection process (as well as residence permit/long-stay visa process, return and removal process, and border-crossing process) for 100 years after the date of birth of the person concerned. Latvia stores biometric data in the national visa information system for 10 years and in the civil and criminal data array for 10 years after the person's death for the international protection process, or 75 years after the date of first entry for the long-stay visa and residence permit process. Within individual Member States, the approach may differ significantly between different processes. For example, in Hungary, data collected for international protection are stored for 15 years, data for long-stay visa requests or collected during the border-crossing process are kept for a maximum of five years, and data collected during the return and removal process are kept for three years. In France, the timeline for storage depends on the type of data collected and the use of these data (e.g. five years after the expiry of the residence permit or travel document, provided there has been no update in the meantime; 30 years for data relating to a deportation order after the measure or sentence is entered in the data processing system if the file has not been updated in the last five years; five years after the expiry of an entry ban; five years for data related to visa applications).

Some EMN Member and Observer Countries have different storage rules depending on the process or content of the data. For example, Finland specifies that biometric data taken for the purpose of comparison may only be used for the duration of the comparison and must be destroyed immediately thereafter. In the Netherlands, when live scans of fingerprints are taken, they are compared to existing fingerprints in the database but are not stored.

Data controller for the collection and processing of biometric data under national legislation

The most common data controllers identified by the EMN Member and Observer Countries are the Ministry of the Interior,[54] an Immigration or Asylum Authority,[55] the police,[56] and the Ministry of Foreign Affairs.[57] Other data controllers included the Ministry of Justice and Security,[58] administrative courts at federal level,[59] or a Parliamentary Commission for Human Rights.[60]

6. PROCESSING OF BIOMETRIC DATA FOR A PURPOSE OTHER THAN THE INITIAL PURPOSE

The inform examines whether the national legislation of EMN Member and Observer Countries allows processing of biometric data for other purposes, such as law enforcement or national security, and whether national legislation or administrative practice allow biometric data stored in a national data repository to be used in SIS alerts.

Processing of biometric data for law enforcement, national security or other purposes

Twenty-two countries indicated that their national legislation permitted the use of biometric data for some other purpose, in line with appropriate safeguards, including national security, criminal or civil investigation, or

53 Act no 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties.
54 AT, BG, CZ, FR, HR, IE, LT, LV, SI, SK.
55 AT, CY, ES, FI, FR, SE and NO.
56 AT, CY, EE, EL, ES, FI, IE, IT, PL, SI. In Ireland, An Garda Síochána (national pólice) are the business owner of the Automated Fingerprint Identification System (AFIS), There is a controller/processor agreement in place with Forensic Science Ireland to process the fingerprints.
57 CZ, FR, PL, SI.
58 NL.
59 AT.
60 UA.

counterterrorism.[61] Four countries reported that biometric data can be used to identify missing persons, deceased persons, or victims of a natural disaster, major accident, or other disaster.[62] In Croatia, biometric data collected during the return process may be used to prevent, detect, and investigate criminal offences relating to terrorism or other serious criminal offences. Finland similarly allows biometric data collected under its Aliens Act, including biometric data collected for the purposes described above and stored in a register maintained by the police, to be used for purposes other than the initial purpose only where strictly necessary for the purposes of preventing, detecting, or investigating criminal offences relating to national security. In Latvia, according to the law, specific institutions may process biometric data originally collected for other purposes in certain cases, including police or administrative bodies associated with the investigation and processing of civil and criminal offences.

Four countries identify criminal investigation, law enforcement, security or national security as an initial purpose for collecting biometric data during the specific migration processes examined.[63] As such, in some cases, the processing of biometric data for criminal investigations or for the purpose of national security does not represent use of biometric data for a secondary purpose. Finnish legislation, for example, explicitly includes national security as an initial purpose for collecting and processing data during the migration processes provided for under the Act on the Processing of Personal Data in Immigration Administration, the Aliens Act, and the Act on the Processing of Personal Data by the Police.

Responding EMN Member and Observer Countries also identified limitations on access to and use of biometric data processed for these additional purposes. In Ireland, any processing of these biometric data for national security, defence, or public security must be necessary and proportionate and must have a clear statutory basis. In Austria, biometric data stored in the Central Aliens Register may be transmitted to specific recipients for specific purposes. The potential recipients of this data are explicitly identified in the same legal framework that creates the Central Aliens Register and biometric data can only be transferred to these recipients if necessary to fulfil specific tasks identified by law under Article 29 (1) of the Federal Office for Immigration and Asylum Procedures Act. The authorities that may receive this data include security authorities, public prosecution authorities, civil and criminal courts, prisons, administrative courts of the federal states, the federal administrative court, and Austrian diplomatic and consular authorities.

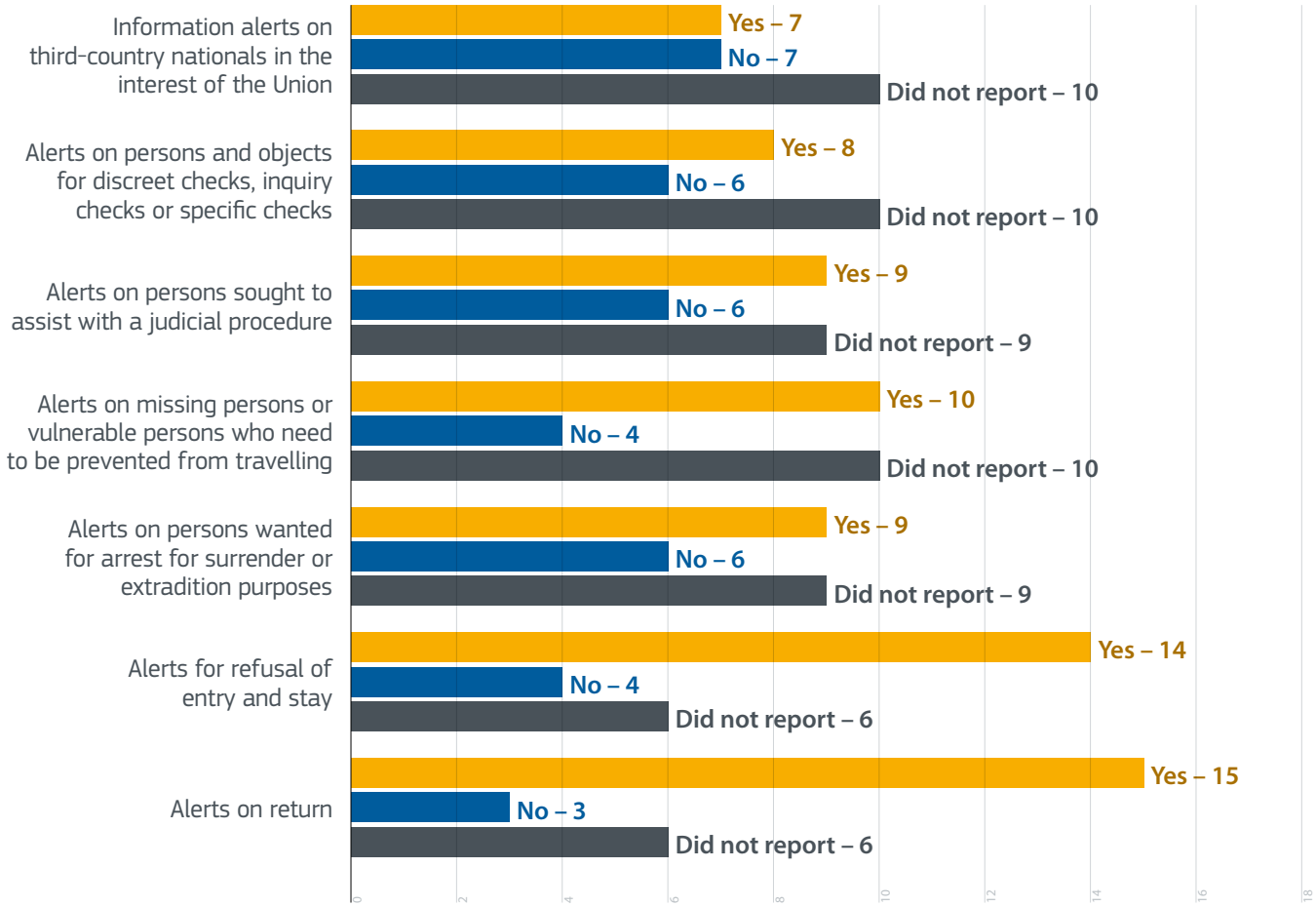
Processing of biometric data for SIS alerts

Responding countries reported on the processing of biometric data for seven specific categories of SIS alerts.[64] Of the responding countries to which SIS alerts apply,[65] 18 allow biometric data collected during the migration processes considered for this inform to be used for SIS alerts.[66] Only seven note that the biometric data may be used for all categories of SIS alerts,[67] with most allowing biometric data to be used only for specific categories of SIS alerts. In Finland, biometric data can only be used for alerts on missing persons or vulnerable persons who need to be prevented from travelling.[68] In France, SIS is interconnected with several national applications: the processing of personal data relating to passports and national identity cards (*fichier des titres électroniques sécurisés* - TES), the Wanted Persons File (*fichier relative aux personnes recherchées - FPR*), the France Visas processing system and the processing system for third-country national residence permits (Application for the Management of the files of third-country nationals in France – AGDREF 2). Some applications consult and feed the SIS, while others merely consult it (France Visas, AGDREF).

Figure 3 presents an overview of the use of biometric data for each type of SIS alert.

61 AT, BE, BG, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE and NO, UA, RS.
62 FI, LV, PL and NO.
63 BE, CZ, HR, FI.
64 Alerts on return (Regulation (EU) 2018/1860), alerts for refusal of entry and stay (Regulation (EU) 2018/1861), alerts on persons wanted for arrest for surrender or extradition purposes (Article 26, Regulation (EU) 2018/1862), alerts on missing persons or vulnerable persons who need to be prevented from travelling (Article 32, Regulation (EU) 2018/1862), alerts on persons sought to assist with a judicial procedure (Article 34, Regulation (EU) 2018/1862), alerts on persons and objects for discreet checks, inquiry checks or specific checks (Article 36, Regulation (EU) 2018/1862), information alerts on third-country nationals in the interest of the Union (Article 37a, Regulation (EU) 2018/1862).
65 SIS alert system applies to all EMN Member Countries and Norway.
66 AT, BE, CZ, DE, EE, ES, FI, FR, HR, HU, IT, LT, LV, NL, PL, SE, SK and NO.
67 CZ, DE, EE, ES, HU and NO.
68 Regulation (EU) 2018/182, Article 32.

Figure 3: Use of biometric data for SIS alerts



Source: EMN Member and Observer Countries

The use of biometric data stored in national repositories for SIS alerts varies widely between the different categories of alerts. The most common categories of alerts for which biometric data can be used are alerts on return (Regulation (EU) 2018/1860)[69] and alerts for refusal of entry and stay (Regulation (EU) 2018/1861).[70] Fifteen countries specify that biometric data stored in national repositories can be used for alerts on return, and 14 for alerts on refusal of entry and stay.

7. INTERNATIONAL TRANSFER OF BIOMETRIC DATA

Of the 27 responding EMN Member and Observer Countries, 22 state that biometric data collected during the relevant migration processes can, to some extent and under certain circumstances, be transferred to third countries (in the case of EU Member States), other countries (in the case of Observer Countries), or to international organisations.[71] Only three countries stated that biometric data could not be transferred.[72]

Although most countries indicated that international transfer of biometric data is permissible, it is typically limited to specific uses or situations. These specific uses vary in nature, but most commonly enable transfer only where required under some form of international legal obligation, such as compliance with EU law or a treaty. For example, four countries have reported that this data may be shared specifically under the VIS and Eurodac Regulations.[73] Data-sharing, including biometric data, for immigration purposes takes place between Ireland and the United Kingdom (UK) in the context of Common Travel Area (CTA) cooperation.[74] In Slovenia, in principle, biometric data cannot be transferred to third countries or international organisations. However, there are some specific derogations from this general rule, including the transfer of data under the VIS and Eurodac regulations.

69 AT, BE, CZ, DE, EE, ES, HR, HU, LT, NL, PL, SE, SK and NO.
70 AT, BE, CZ, DE, EE, ES, HU, IT, LT, NL, PL, SE, SK and NO.
71 AT, BE, BG, CY, DE, ES, FI, FR, HU, HR, IE, IT, LT, LV, NL, PL, SE, SI, SK and NO, UA, RS.
72 CZ, EL, PT.
73 CY, IT, SI and NO.
74 The CTA is a long-standing arrangement between Ireland and the UK, enabling Irish and UK citizens to travel and reside in either jurisdiction without restriction and providing for associated rights and entitlements in both jurisdictions. Immigration authorities in both jurisdictions cooperate to protect the borders of the CTA and prevent its abuse.

Ten countries allow such data-sharing as part of the return or removal process.[75] In Croatia and the Netherlands, biometric data collected during migration process cannot be transferred internationally. However, data collected during the removal and return process may be transferred for the purpose of completing the removal and return process to the country of return, as well as to a transit country during travel for forced removal. Four EMN Member Countries report that fingerprints can be shared in the implementation of certain readmission agreements.[76]

For persons of legal age, Spain generally allows international transfer of biometric data to international organisations and third countries under the terms established in the treaties and conventions to which Spain is a party, such as Interpol, Europol, SIS, EU, European Union, and bilateral agreements. However, data collected from minors may only be transferred to foreign public institutions in charge of protection of minors, or to organisations designated in Spain's national legislation.[77]

75 BE, ES, FI, HR, IE, IT, NL, SE, SK and RS.
76 ES, IE, IT, SK.
77 Organic Law 3/2018; Organic Law 7/2021.

For more information

EMN website: http://ec.europa.eu/emn
EMN LinkedIn page: https://www.linkedin.com/company/european-migration-network
EMN X account: https://x.com/emnmigration
EMN YouTube channel: https://www.youtube.com/@EMNMigration

EMN National Contact Points

Austria www.emn.at/en/
Belgium www.emnbelgium.be/
Bulgaria www.emn-bg.com/
Croatia emn.gov.hr/
Cyprus www.moi.gov.cy/moi/crmd/emnncpc.nsf/home/home?opendocument
Czech Republic www.emncz.eu/
Estonia www.emn.ee/
Finland emn.fi/en/
France www.immigration.interieur.gouv.fr/Europe-et-International/Le-reseau-europeen-des-migrations-REM3/Le-reseau-europeen-des-migrations-REM2
Germany www.bamf.de/EN/Themen/EMN/emn-node.html
Greece https://migration.gov.gr/emn/
Hungary www.emnhungary.hu/en
Ireland www.emn.ie/
Italy www.emnitalyncp.it/
Latvia www.emn.lv
Lithuania www.emn.lt/
Luxembourg emnluxembourg.uni.lu/
Malta emn.gov.mt/
The Netherlands www.emnnetherlands.nl/
Poland www.gov.pl/web/european-migration-network
Portugal rem.sef.pt/en/
Romania www.mai.gov.ro/
Spain www.emnspain.gob.es/en/home
Slovak Republic www.emn.sk/en
Slovenia emnslovenia.si
Sweden www.emnsweden.se/
Norway www.udi.no/en/statistics-and-analysis/european-migration-network---norway#
Georgia migration.commission.ge/
Republic of Moldova bma.gov.md/en
Ukraine dmsu.gov.ua/en-home.html
Montenegro www.gov.me/mup
Armenia migration.am/?lang=en
Serbia kirs.gov.rs/eng