European Commission

European Migration Network

ACCURATE, TIMELY, INTEROPERABLE? DATA MANAGEMENT IN THE ASYLUM PROCEDURE

EMN INFORM 2021

A smooth and fast registration and identification procedure that maintains data accuracy is an essential aspect of a functioning asylum procedure. Several Member States and Norway recently adopted a wide range of measures to improve interoperability to assist operational efficiency and enable European Union (EU) information systems to complement one another.

Recent years have seen changing circumstances in applications for international protection, with increases and decreases in the volume and types of applications, prompting procedural changes in the asylum process, impacting how personal data are collected, managed and shared in several Member States and Norway. Most recently, the outbreak of the COVID-19 pandemic in early 2020 has also impacted on data management in asylum procedures.

This Inform summarises the results of the EMN study of the same title which examines how data are managed in the different phases of the asylum procedure (making, registering, lodging and examining) across the Member States and Norway. It maps data management approaches in the asylum procedure, examines challenges faced by Member States, and analyses the impact of any procedural changes to enhance data-sharing among asylum authorities (and others).

KEY POINTS TO NOTE

1. **Member States collect different types of data as part of the asylum procedure. However, some categories of data are commonly collected by most, if not all, Member States and Norway**, including data on current and/or birth names, birth date, citizenship, contact details, health status, photo and fingerprints, information on family members already in a Member State, vulnerabilities, and level of education.
2. Frontloading data collection is considered good practice by some Member States, as it allows authorities to access applicants' information in the early phase of the asylum procedure and to prioritise certain categories of applications. Frontloading may also save on administrative capacity and facilitate other competent institutions' immediate access to data. **A trend in frontloading data collection was observed for basic personal data (e.g. name, biometrics, place of birth) and supporting documents (e.g. passport and travel documents).** As a result, an increasing amount of data is collected by border guards and local police, as the main authorities responsible for registering and lodging applications in most Member States.
3. **Data on asylum applicants are primarily collected through oral interviews, questionnaires and electronic tools (for biometric data). However, several Member States have also started to use social media analysis, analysis of mobile devices and artificial intelligence (AI) to collect data on asylum applicants**. Most data collected in the asylum procedure is stored in databases. In some cases, Member States use a combination of databases, electronic files and paper files to store data, but this approach may cause certain inefficiencies in data management. The increased digitalisation of data management and the use of centralised databases to store asylum applicants' data is seen as good practice by several Member States.
4. **Most Member States and Norway cross-check data on asylum applicants against European (i.e. Visa Information System (VIS), Schengen Information System (SIS), Eurodac) and national databases. Only a minority cross-check information against international databases**. Most cross-checks happen during the lodging phase.
5. **EU data protection legislation requires Member States to have safeguards in place to ensure respect for the right to data protection. Member States and Norway have implemented several data safeguards in the asylum procedure,** such as providing a privacy notice to applicants, assessing the quality of data collected in the asylum procedure, and implementing data protection supervisory and compliance mechanisms.
6. **Since 2014, most Member States have experienced challenges in data management. These challenges primarily relate to the lack of human or financial resources and the interoperability of (national) databases**. Member States have faced technical limitations in data processing (e.g. old equipment, lack of technical capacity), issues related to transliteration, and challenges related to the implementation of the General Data Protection Regulation (GDPR).
7. **Changes introduced by Member States** in response to these challenges include **consolidating databases to increase interoperability, channelling asylum applications to prioritise certain cases, and implementing contingency measures to ease the asylum process in times of high numbers of applicants.**
8. **Some Member States changed their data management procedures in response to challenges to the implementation of asylum processes posed by the COVID-19 pandemic, including the digitalisation of some steps of the asylum procedure and changes in the collection of fingerprints.**

DG Migration & Home Affairs

EMN European Migration Network

SCOPE AND AIMS OF THE STUDY

The study examines how data are managed in the different phases of the asylum procedure (making, registering, lodging and examining) across the Member States and Norway. It maps data management approaches in the asylum procedure (i.e. data protection and safeguards), examines challenges faced by Member States, and analyses the impact of any procedural changes to enhance data-sharing among asylum authorities (and others).

The study reflects the situation and developments in data management in the asylum procedure between 2014 and 2020, the initial three years of which were characterised by very high numbers of applicants for international protection (Figure 1).[1] The impact of the COVID-19 pandemic on data management in the asylum procedure is also briefly explored. As regards statistics, the period 2014-2019 is covered.

The study refers to the different phases of the asylum procedure, as defined by the European Asylum Support Office (EASO):[2]

- **Making an application:** the person expresses their intention to apply for international protection ('making' phase);
- **Registering an application:** the applicant's intention to seek protection is registered, which may be done by an authority not competent for the asylum procedure itself, such as border police ('registering' phase);
- **Lodging an application:** the asylum application is formally lodged with the competent authority for the asylum procedure ('lodging' phase);
- **Examining the application** ('examining' phase).

METHOD AND ANALYSIS

The information used in this report is drawn from national reports from 24 Member States and Norway,[3] developed according to a common data collection template. National contributions were based on desk analysis of existing legislation and policy documents, reports, academic literature, internet resources, media reports and information from national authorities. In some Member States, primary data collection was carried out through interviews with national stakeholders.

THE ASYLUM PROCEDURE

EASO distinguishes four main procedural phases in asylum-seeking: making, registering, lodging and examining an application.[4] Most Member States provide for a clear legal distinction between the first three phases of the asylum procedure (making, registering and lodging). Four Member States make a clear legal distinction between those phases but do not differentiate between them in practice.[5] A minority of Member States, as well as Norway, do not differentiate between the first three phases in either law or practice.

The time that it takes from making an asylum application until a first-instance decision is issued varies across the EU and Norway. After 2014, a number of Member States introduced or changed the specific time limits in legislation for the different phases of the asylum procedure (from making to examining an application). In practice, the average time from making an asylum application to the lodging of the application in the ordinary procedure varies considerably, ranging from a few days to several months. Similarly, the average time needed to issue a first-instance decision after lodging an asylum application also varies significantly between Member States in practice. In order to accelerate or prioritise some asylum applications, most Member States have introduced formal/informal channelling systems, for example applications by third-country nationals coming from a safe country of origin, or by vulnerable groups, or applications that are manifestly unfounded.

Several Member States have adopted a decentralised system, with more than one authority involved in one or several phases of the asylum procedure. However, eight Member States and Norway follow a more centralised system, with a single authority responsible for each phase.[6] Border guards and local police are involved in the making, registering and lodging phases in most Member States, while the examining phase is chiefly conducted by the competent ministry, the immigration office, or the office for refugees. In several Member States, authorities in detention facilities and reception centres are also involved in the asylum procedure, although primarily in the making phase.

Although there are some differences in the type of data collected across the EU, certain categories of data are commonly collected by most, if not all, Member States and Norway. For example, all collect data on the asylum applicant's current name, contact details, family members and health status, as well some categories of biometric data (photo and fingerprints). Data on education, vulnerabilities and family members already present in Member States are also collected by most Member States. A trend in frontloading the collection of some elements of asylum applicants' data was observed for some categories of data, including: name, biometrics, place of birth and supporting documents (e.g. passport, travel documents). This trend in frontloading means that an increased amount of data is collected by border guards and local police officers in most Member States, as the main authorities involved in the registering and lodging phases.

Data collection and data management in the asylum procedure are increasingly digitalised, although 'traditional' data collection and storage methods remain the primary tools used by Member States. Asylum applicants' information is mainly collected through oral (face-to-face) interviews and questionnaires, and, for biometric data, electronic tools. Eight Member States and Norway also use new methods

1 Reaching a peak of more than 1.3 million asylum applications in the EU and Norway in 2015.

2 EASO, 'Guidance on asylum procedure: operational standards and indicators', September 2019, https://easo.europa.eu/sites/default/files/Guidance_on_asylum_procedure_operational_standards_and_indicators_EN.pdf, last accessed on 28 May 2021.

3 AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SE, SI, SK and NO.

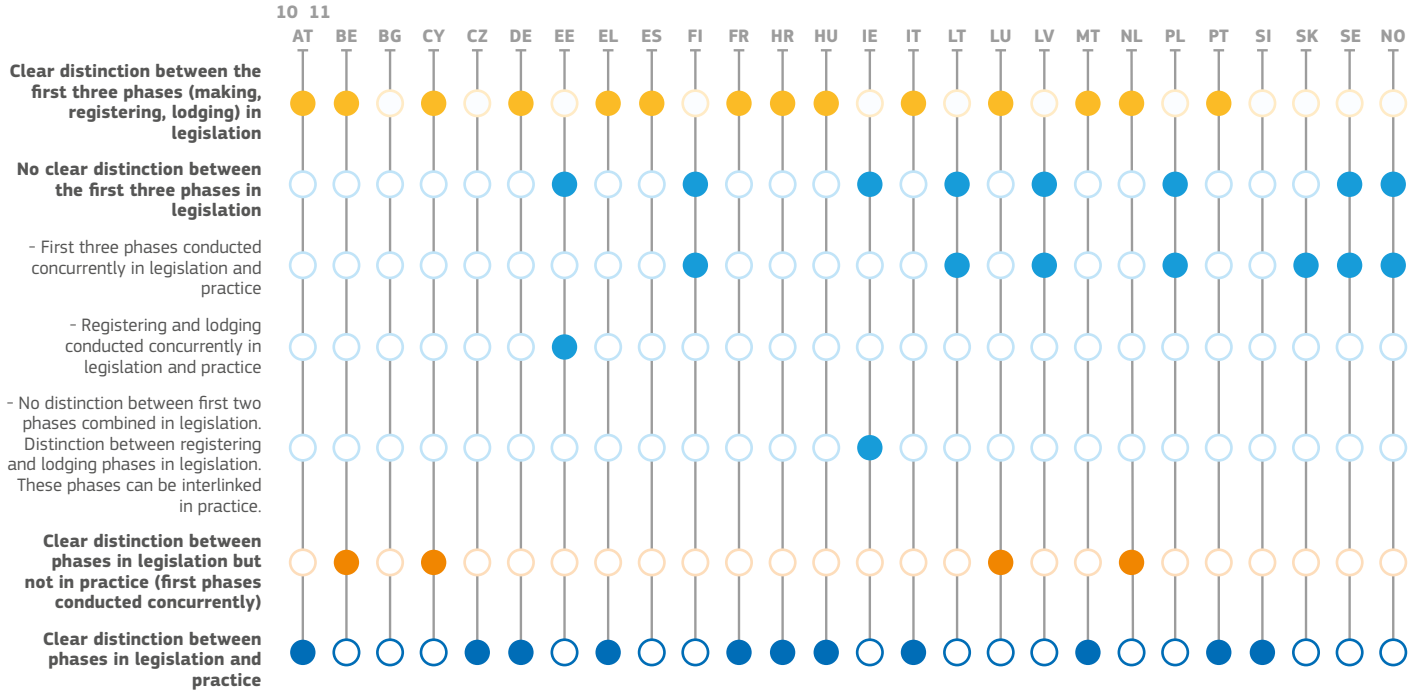
4 EASO, 'Guidance on asylum procedure: operational standards and indicators', September 2019, https://easo.europa.eu/sites/default/files/Guidance_on_asylum_procedure_operational_standards_and_indicators_EN.pdf, last accessed on 28 May 2021.

5 BE, CY, LU, NL.

6 EE, EL, HR, IE, IT, PL, SE, SK and NO.

and technologies to collect data on asylum applicants (e.g. social media analysis, analysis of mobile devices, AI).[7] Twenty Member States and Norway store asylum applicants' data in databases[8] and 15 Member States also use paper files.[9] Data on asylum applicants stored in databases can in most cases, be accessed or shared with different authorities involved in the asylum procedure. In several Member States and Norway, access to either specific databases or specific categories of data is sometimes granted to institutions outside the asylum procedure (e.g. health authorities, labour authorities, intelligence services) for purposes other than the asylum procedure.

Figure 1. Overview of phases in Member States and Norway



KEY ASPECTS OF DATA MANAGEMENT ACROSS THE PHASES OF THE ASYLUM PROCEDURE

In most Member States, authorities who are not competent to register applications for international protection nevertheless have a role in data management in the asylum procedure. They may provide information to applicants on the registration process and/or direct the person to the competent authority, for example. In several Member States, non-competent authorities are also required to directly inform the competent authority of a third-country national's intention to apply for asylum. Eleven Member States noted that no data are collected during the making phase by authorities without the competence to register applications for international protection.[12] Seven Member States allow some non-competent authorities to collect data on asylum applicants (e.g. basic personal information, fingerprints) and transfer that information to the competent national authorities.[13]

Most Member States cross-check data on asylum applicants against national and European (i.e. SIS, VIS and Eurodac) databases at some stage of the asylum procedure. Few Member States cross-check data on asylum applicants against international databases (e.g. Interpol Stolen and Lost Travel Documents (SLTD)). The most commonly checked national databases include registers for wanted persons, criminal record databases, security databases, immigration databases, databases with information on entry bans, and national fingerprints databases. Most cross-checks are carried out during the lodging phase, although several Member States cross-check data against national, European and international databases in more than one phase of the asylum procedure. Several Member States reported facing issues when cross-checking data against databases, including problems with transliteration, rules applicable to different databases, and inaccurate or insufficient information in the databases.

7 BE, DE, EL, FI, FR, LT, NL, PT and NO.
8 AT, BE, CY, CZ, HR, EE, EL, FI, HU, FR, IE (data collected and recorded at registering and lodging stage is recorded electronically, printed and placed in a paper file), IT, LT, LU, LV, NL, PL, PT, SK, SE and NO.
9 CY, CZ, EE, EL, FR, HR, HU, IE, IT, LU, LT, LV, MT, PL, SK.
10 AT has no distinct registering phase.
11 Ibid.
12 AT, EE, FI, HR, LU, LV, NL, PT, SE, SI, SK.
13 CZ, DE, FR, HU, IE, IT, MT.

Most Member States and Norway provide asylum applicants with a privacy notice containing information on personal data collected and processed as part of the asylum procedure. The privacy notice may be provided during the lodging phase (20 Member States and Norway),[14] the examining phase (13 Member States)[15] and/or the registering phase (12 Member States).[16] The information contained in the privacy notice is usually provided in writing and/or verbally, although several Member States and Norway also provide it digitally. In most cases, whenever a privacy note is provided, translation and interpretation are also offered.

About half of the Member States and Norway provide specific training or guidance on data protection to staff responsible for data management in the different phases of the asylum procedure.

Table 1. Type of databases cross-checked by Member States in the different phases of the asylum procedures

	Registering phase	Lodging phase	Examining phase
National databases	BE, CY, CZ, DE, EE, FR, HR, IE, IT, MT, NL,[164] SE, SI	AT, CY, DE, EE, ES, FI, FR, HR, HU, LT, LU, LV, NL, PL, PT, SE, SI, SK and NO	AT, CY, EE, ES, FI, HR, HU, LT, LV, PT, SE, SK
European databases	BE, CY, CZ, DE, EE, EL, FR, HR, IE, IT, MT, NL, SE	AT, CY, DE, EE, EL, ES, FI, HR, HU, LT, LU, LV, MT, NL, PL, PT, SE, SI, SK and NO	EE, EL, ES, FI, HR, HU, LV, PT, SK and NO
- SIS	BE, CZ, DE, EE, EL, HR, IT, MT, NL, PT, SE, SI	AT, DE, EE, EL, FI, HR, LU, LV, MT, NL, PL, PT, SE, SK and NO	EE, EL, ES, FI, HR, LT, LV, PT, SE, SK and NO
- VIS	BE, CZ, DE, EE, EL, IT, MT, NL, PT, SE	AT, DE, EE, EL, FI, LU, LV, MT, NL, PL, PT, SE, SK and NO	EE, EL, ES, FI, LT, LV, PT, SE, SK and NO
- Eurodac	BE, CY, CZ, DE, EL, FR, HR, IE, IT, NL, PT, SE, SI	AT, CY, ES, FI, FR, HR, IT, NL, LU, LV	
International databases (e.g. Interpol SLTD)	CY, CZ, HR, PT, SI	CY, LU, LV, NL, PT, SK and NO	EE, LT, LV, PT, ES

DATA QUALITY ASSESSMENT AND SAFEGUARDS

The vast majority of the Member States and Norway assess the quality of alphanumeric and biometric data collected during the asylum procedure for accuracy, timeliness, completeness, consistency, duplication and validity. Those quality checks are generally carried out during one or more phases of the asylum procedure. However, in four Member States, quality checks are only retroactive.[18] National competent authorities use a wide range of quality control tools and methods to assess the quality of data processed during the asylum procedure, such as automatic quality checks, carrying out data comparisons across different datasets, and involving applicants in quality checks. In addition, most Member States and Norway have preventive measures in place to ensure the collection of the correct data, for example by including mandatory fields or predefined fields with drop-down lists in databases. The collection of incorrect data may be further prevented through guidance and training for the staff involved.

To ensure the lawfulness of data processed as part of the asylum procedure, Member States and Norway have established data protection supervisory and compliance mechanisms. In 11 Member States and Norway,[19] the data protection supervisory mechanism applicable to the asylum procedure is part of the general national data protection supervision procedures entrusted to the national Data Protection Authority (DPA), while four Member States have a specific data protection supervision and compliance mechanism under the competence of migration authorities.[20] Five Member States use a combination of the two systems.[21] A number of Member States have already undergone assessments of the lawfulness of personal data processing in the context of the asylum procedure, which tended to lead to changes and improvements in data management.

According to the GDPR, asylum applicants can request to access, erase, and rectify their data. Depending on the Member State, the request to access, erase or rectify data can be made in person, electronically or by post. Asylum seekers are usually required to present proof of identity and, in the case of rectification, justification for the changes. In line with the exceptions foreseen under the GDPR, several Member States do not allow the erasure of data - or some categories of data - related to asylum applicants (e.g. for archiving purposes).

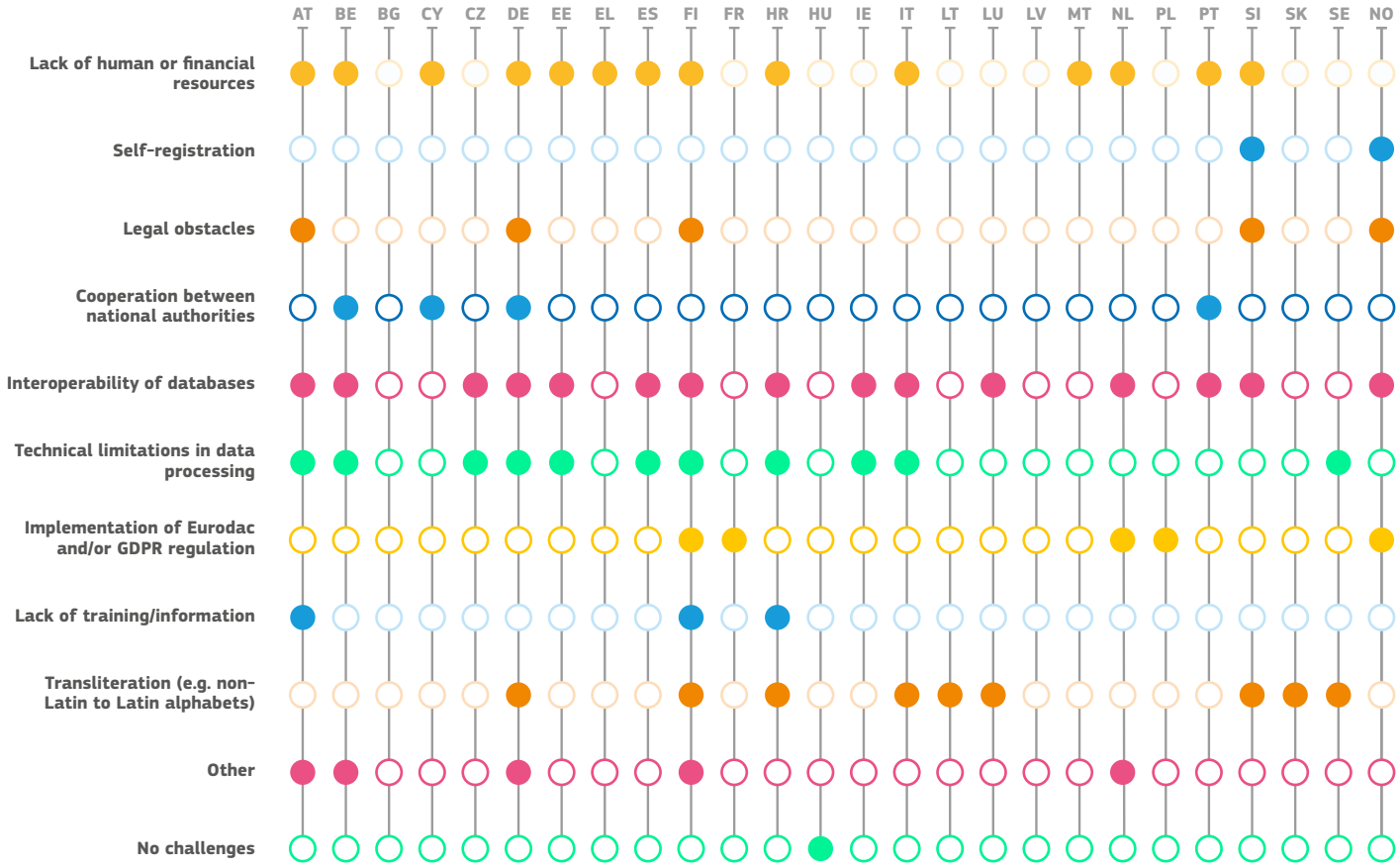
14 AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE, SI, SK and NO.
15 CY, DE, EL, FI, FR, HR, IT, LT, LV, NL, PT, SE, SK.
16 CZ, DE, EE, EL, ES, FR HR, HU, IT, NL, PT, SE.
17 In NL, the registering and lodging phases are combined (see section 3.3).
18 FR, HU, NL, SE.
19 BE, HR, CY, CZ, HU, IE, IT, LT, PT, SI, SK and NO.
20 AT, EE, FI, PL.
21 DE, ES, LU, NL, SE.

CHALLENGES IN DATA MANAGEMENT

Since 2014, the majority of the Member States and Norway have experienced a number of challenges related to data management in the asylum system. The most common challenges relate to the lack of human or financial resources and the interoperability of national and/or EU databases, for example when databases are managed by different authorities, or different formats (e.g. paper and electronic) are used across systems. Twelve Member States also reported challenges related to technical limitations in data processing (e.g. old equipment, lack of technical capacity)[22] and eight Member States experienced issues with transliteration from Cyrillic or Arabic to Latin, which may hinder cross-checking of data.[23]

Some of these challenges are ongoing in 14 Member States and in Norway, with several others exploring different solutions.[24]

Figure 2. Overview of challenges



22 AT, BE, CZ, DE, EE, ES, FI, HR, IE, IT, SE, SI.
23 FI, HR, IT, LT, LU, SE, SI, SK.
24 BE, CY, CZ, DE, FI, HR, IE, LU, LV, MT, NL, PT, SE, SI and NO.

RECENT DEVELOPMENTS IN RELATION TO DATA MANAGEMENT

Since 2014, several Member States and Norway have responded to data challenges by introducing changes to data management in the asylum procedure. Most of those changes relate to the digitalisation of data management, the adequate implementation of the GDPR, and database re-organisation (e.g. introduction of new databases or changes to existing ones). Most of these changes were considered good practices by Member States and have become standard operating procedures.

Eleven Member States and Norway have adopted contingency measures for data management, seeking to accelerate and ease the process at times of high influx of applicants, while also making the asylum systems crisis-proof. [25] Those contingency measures include the possibility to introduce modifications to some of the phases of the asylum procedure to reduce pressure in times of high influx, as well as the adoption of contingency plans.

The COVID-19 pandemic led to changes in data collection and management in eight Member States and Norway. [26] Changes included the temporary suspension of the registration of asylum applications and changing the procedure for collecting fingerprints to minimise physical contact. Member States took action to digitalise certain aspects of the asylum procedure, such as setting up remote interviews or creating digital platforms for administrative actions. In other cases, the digitalisation of the asylum procedure was accelerated by the pandemic.

FULL STUDY PUBLICATION

The full study publication can be accesssed here:

https://ec.europa.eu/home-affairs/content/emn-study-data-management-asylum-procedure_en

25 AT, CZ, DE, EL, FI, FR, IT, LV, NL, SE, SI and NO.

26 BE, DE, EL, FI, HR, LT, NL, SE and NO.

Keeping in touch with the EMN

EMN website www.ec.europa.eu/emn
EMN LinkedIn page www.linkedin.com/company/european-migration-network/
EMN Twitter www.twitter.com/EMNMigration

EMN National Contact Points

Austria www.emn.at
Belgium www.emnbelgium.be
Bulgaria www.emn-bg.com
Croatia https://emn.gov.hr/
Cyprus www.moi.gov.cy
Czech Republic www.emncz.eu
Denmark https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/authorities/denmark_en
Estonia www.emn.ee
Finland www.emn.fi
France www.immigration.interieur.gouv.fr/Europe-et-International/Le-reseau-europeen-des-migrations-REM2
Germany www.emn-germany.de
Greece www.emn.immigration.gov.gr/el/
Hungary www.emnhungary.hu
Ireland www.emn.ie
Italy www.emnitalyncp.it
Latvia www.emn.lv
Lithuania www.emn.lt
Luxembourg www.emnluxembourg.lu
Malta https://homeaffairs.gov.mt/en/mhas-information/emn/pages/european-migration-network.aspx
Netherlands www.emnnetherlands.nl
Poland www.emn.gov.pl
Portugal https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/authorities/portugal_en
Romania www.mai.gov.ro
Slovak Republic www.emn.sk
Slovenia www.emm.si
Spain http://extranjeros.empleo.gob.es/en/redeuropeamigracion
Sweden www.emnsweden.se

Georgia www.migration.commission.ge

Moldova www.bma.gov.md/en
Norway www.emnnorway.no

DG Migration & Home Affairs