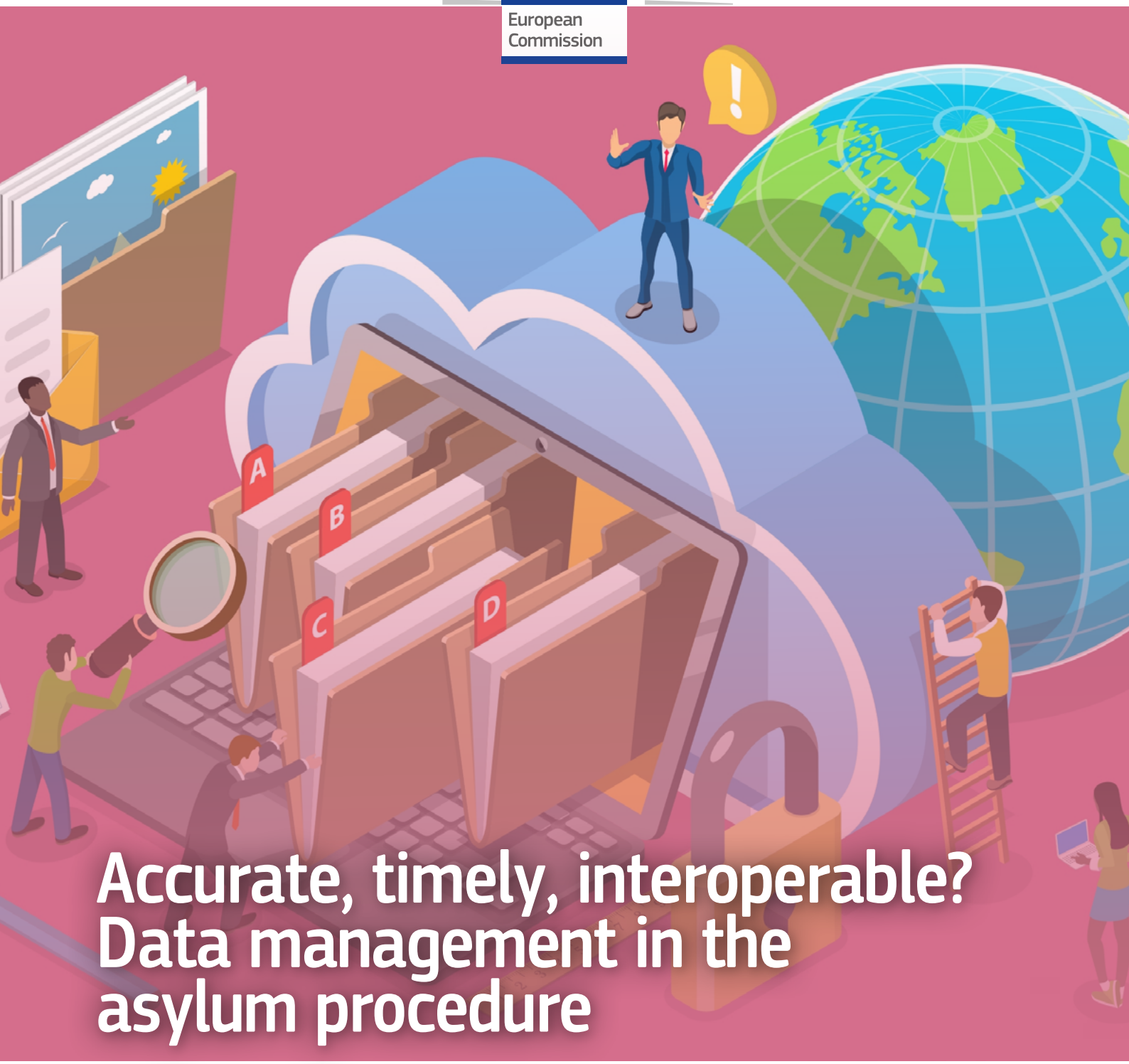
European Commission



Accurate, timely, interoperable? Data management in the asylum procedure

EMN Study June 2021

EMN
European Migration Network

Disclaimer

This study has been produced by the European Migration Network (EMN), which comprises the European Commission, its Service Provider (ICF) and EMN National Contact Points (EMN NCPs). The report does not necessarily reflect the opinions and views of the European Commission, EMN Service Provider (ICF) or the EMN NCPs, nor are they bound by its conclusions. Similarly, the European Commission, ICF and the EMN NCPs are in no way responsible for any use made of the information provided.

The study was part of the 2020 work programme for the EMN.

Suggested citation

European Migration Network (2021). Accurate, timely, interoperable? Data management in the asylum procedure – study. Brussels: European Migration Network.

Explanatory note

This study was prepared on the basis of national contributions from 25 EMN NCPs (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) according to a common template developed by the EMN and followed by EMN NCPs to ensure, to the extent possible, comparability.

National contributions were largely based on desk analysis of existing legislation and policy documents, reports, academic literature, internet resources and reports and information from national authorities. Statistics were sourced from Eurostat, national authorities and other (national) databases. The listing of Member States in the study results from the availability of information provided by the EMN NCPs in their national contributions.

It is important to note that the study reflects the situation and developments between 2014 and 2020, including the years 2014 to 2016, which were characterised by very high numbers of applicants for international protection. The impact of the COVID-19 pandemic on data management in the asylum procedure is also briefly explored. Statistics used in the study cover the period 2014-2019. More detailed information on the topics addressed here may be found in the available national contributions and it is strongly recommended that these are consulted as well.

EMN NCPs from other Member States could not, for various reasons, participate on this occasion in this study, but have done so for other EMN activities and reports.

CONTENTS

EXECUTIVE SUMMARY ____ **4**

1. INTRODUCTION ____ **9**

1.1. STUDY AIMS ____ 9

1.2. SCOPE OF THE STUDY ____ 10

1.3 RATIONALE AND EU POLICY CONTEXT ____ 12

1.4 STRUCTURE OF THE REPORT ____ 12

2. THE ASYLUM PROCEDURE ____ **14**

2.1. OVERVIEW OF THE ASYLUM PROCEDURE ____ 14

2.2. OVERVIEW OF AUTHORITIES INVOLVED IN THE ASYLUM PROCEDURE ____ 15

2.3 DATA COLLECTED DURING THE ASYLUM PROCEDURE ____ 14

2.4 OVERVIEW OF DATA MANAGEMENT IN THE ASYLUM PROCEDURE ____ 14

3. KEY ASPECTS OF DATA MANAGEMENT ACROSS THE PHASES OF THE ASYLUM PROCEDURE ____ **17**

3.1. MAKING AN APPLICATION FOR INTERNATIONAL PROTECTION TO AN AUTHORITY NOT COMPETENT TO REGISTER THE APPLICATION ____ 17

3.2. REGISTERING AN APPLICATION FOR INTERNATIONAL PROTECTION ____ 21

3.3. LODGING AN APPLICATION ____ 21

3.4. EXAMINING AN APPLICATION ____ 21

4. DATA QUALITY ASSESSMENT AND SAFEGUARDS ____ **26**

4.1. DATA QUALITY MANAGEMENT ____ 26

4.2. DATA PROTECTION SAFEGUARDS: SUPERVISION AND INDIVIDUAL RIGHTS ____ 31

5. CHALLENGES IN DATA MANAGEMENT ____ **37**

6. RECENT DEVELOPMENTS RELATING TO DATA MANAGEMENT ____ **37**

6.1. CHANGES AND REFORMS IN DATA MANAGEMENT ____ 26

6.2. CONTINGENCY MEASURES ____ 31

6.3. IMPACT OF COVID-19 ON DATA MANAGEMENT IN THE ASYLUM PROCEDURE ____ 26

7. CONCLUSIONS ____ **37**

8. ANNEXES ____ **37**

EXECUTIVE SUMMARY

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.**

SCOPE AND AIMS OF THE STUDY

This 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).

This 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.

This 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.

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.

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 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.

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.[10] 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.[11]

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.

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),[12] the examining phase (13 Member States)[13] and/or the registering phase (12 Member States).[14] 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.

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.[15] 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,[16] the data protection supervisory mechanism applicable

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

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.[17] Five Member States use a combination of the two systems.[18] 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).

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)[19] and eight Member States experienced issues with transliteration from Cyrillic or Arabic to Latin, which may hinder cross-checking of data.[20]

Some of these challenges are ongoing in 14 Member States and in Norway, with several others exploring different solutions.[21]

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. [22] 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. [23] 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.

17 AT, EE, FI, PL.
18 DE, ES, LU, NL, SE.
19 AT, BE, CZ, DE, EE, ES, FI, HR, IE, IT, SE, SI.
20 FI, HR, IT, LT, LU, SE, SI, SK.
21 BE, CY, CZ, DE, FI, HR, IE, LU, LV, MT, NL, PT, SE, SI and NO.
22 AT, CZ, DE, EL, FI, FR, IT, LV, NL, SE, SI and NO.
23 BE, DE, EL, FI, HR, LT, NL, SE and NO.

1. INTRODUCTION

1.1. STUDY AIMS

This study examines how data are managed in the different phases of the asylum procedure across the Member States and Norway. It maps data management approaches in the asylum procedure, examines whether there have been procedural changes to enhance data-sharing among asylum authorities (and others), and how such changes have impacted data management. Finally, the study identifies recent trends, challenges and good practices in relation to data management.

The study focuses on answering the following primary questions:

- What information is collected in the context of the asylum procedure, at what point in time, and by whom?
- How is the information collected, fed into different data systems, and further managed and shared with relevant actors?
- How is data quality assessed, and what data protection safeguards are in place for asylum applicants during the asylum procedure?
- What changes did Member States and Norway introduce in recent years with regard to data management in the asylum procedure, and why?
- What challenges do Member States and Norway face in respect of data management in the asylum procedure, how have these been overcome, and what good practices can be shared?

1.2. SCOPE OF THE STUDY

This study is based on national reports from 24 Member States and Norway,[24] developed according to a common template questionnaire. 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, interviews with national stakeholders were carried out.

The study reflects the situation and developments between 2014 and 2020, including the years 2014 to 2016, which were characterised by very high numbers of applicants for international protection. The impact of the COVID-19 pandemic on data management in the asylum procedure is also briefly explored. Statistics used in the study cover the period 2014-2019.

The study addresses data collection in four phases of the asylum procedure, as defined by the European Asylum Support Office (EASO):[25]

- **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).

Not all legal frameworks in the Member States and Norway follow this distinction, however. In several cases, some of these phases are not clearly distinguished in legislation and/or are conducted concurrently in practice.

The study looks at the categories of data collected during the asylum procedure, by what authorities, and at which of the four phases identified above. It also examines where collected data are stored, and if they are shared between databases, or reused. It explores how national authorities ensure data quality and provide safeguards in each of the various phases, and describes the challenges identified by Member States and Norway in relation to data collection and processing and changes and reforms implemented since 2014.

24 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.
25 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.

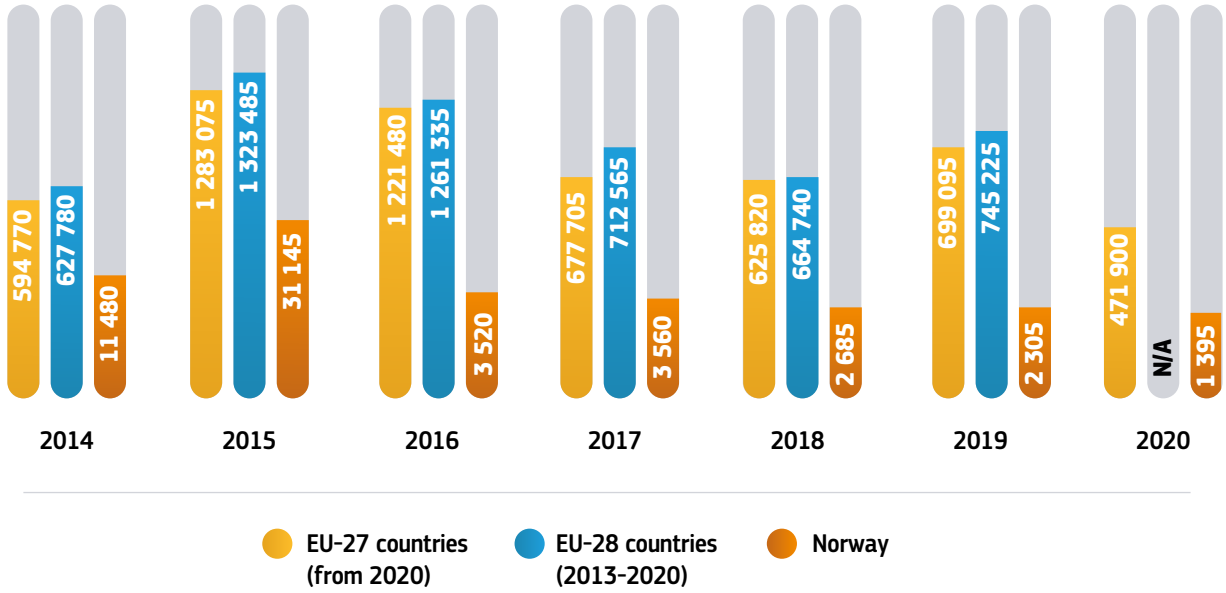
1.3. RATIONALE AND EU POLICY CONTEXT

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.[26]

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

The significant increase in asylum applications in the EU between 2014 and 2016 (Figure 1) presented a challenge to EU Member States and prompted a number of policy developments. For example, during the period of increased arrivals of refugees and migrants in the EU, several Member States struggled with their capacity to register asylum seekers and to manage data across different databases – both within their respective asylum authorities and other authorities linked to the asylum procedure and reception of applicants.[27] Some Member States reported backlogs and delays in data management and expressed their willingness to increase automation, digitalisation and innovation (e.g. through the use of AI[28]). The spike in arrivals of individuals seeking international protection in 2015 resulted in the increased involvement of EASO in the asylum process. EASO provided assistance to some Member States (e.g. Greece) to process asylum requests, as well as lending operational support through the 'hotspot approach' to the frontline Member States most affected by increased arrivals of refugees and migrants.[29]

Figure 1. Total number of asylum applications lodged in the EU and Norway between 2014 and 2020[30]



26 European Parliament, 'Interoperability of Justice and Home Affairs Information Systems, Study for the LIBE Committee', 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf, last accessed on 28 May 2021.

27 EMN, 'Changing Influx of Asylum Seekers 2014-2016, Synthesis Report', 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_changing_influx_study_synthesis_final_en.pdf, last accessed on 28 May 2021.

28 Artificial intelligence (AI) is defined by the EU Commission as referring to the systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications). See Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN, last accessed on 28 May 2021.

29 Tsourdi, E. L., 'Refugee recognition in the EU: EASO's shifting role' (2020), Forced Migration Review, Vol. 65, pp. 29-31, https://www.fmreview.org/recognising-refugees/tsourdi, last accessed on 28 May 2021.

30 Eurostat, total number of asylum applications, migr_asyappctza, extracted on 3 May 2021.

Operational challenges arose from the lack of interoperability between information systems, with data protection issues highlighted at national and EU levels. As a result, several Member States introduced a range of measures to enhance interoperability at national level, or implemented broad data management reform, raising questions about personal data safeguards and legal limitations of data collection and processing mechanisms. The question of interoperability is similarly on the EU agenda. The abolition of internal borders in the Schengen area necessitates strong and reliable management of the movement of persons across external borders, including through robust identity management. Three centralised information systems have been developed by the EU and are currently operational under several regulations (either updated or in the legislative process of being updated): the Schengen Information System (SIS)[31], the Visa Information System (VIS)[32] and Eurodac. [33] All of these information systems assist in verifying or identifying third-country nationals who are on the move and who fall into different categories. SIS, VIS and Eurodac were originally envisaged to operate independently of one another, with no interaction. As these centralised information systems developed, however, the need to provide technical and legal solutions that would enable these systems to 'speak to each other' became clear. To that end, the Interoperability Regulations[34] were adopted in 2019 to provide for a series of tools to enhance interconnection between data stored in different EU information systems. From a privacy and personal data protection perspective, the General Data Protection Regulation (GDPR)[35] was approved and entered into force during the reporting period (May 2018). The GDPR established a unique set of rules for data protection across the Member States and Norway, intended to strengthen individuals' fundamental right to privacy and data protection in the digital age. The GDPR is also applicable to the processing of personal data in the asylum procedure.

1.4. STRUCTURE OF THE REPORT

Section 2 of the report provides an overview of the asylum procedure. It includes the distinction between different phases in Member States and Norway, maps the authorities involved, and information on data collection. **Section 3** looks at data management and the provision of information to asylum applicants in each phase of the asylum procedure – making, registering, lodging and examining. **Section 4** examines data quality assessment and data safeguards applied by the Member States and Norway during the asylum procedure. **Sections 5 and 6** outline recent challenges and changes/reforms in data management, including a brief overview of the impact of COVID-19 on data management and the specific changes introduced by Member States and Norway because of the pandemic. Conclusions from the report are set out in **Section 7.**

31 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, OJ L312, p. 56, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1862, last accessed on 28 May 2021; 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, OJ L312, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1860, last accessed on 28 May 2021; 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, OJ L312, p. 14, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1861&from=EN, last accessed on 28 May 2021.

32 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, OJ L218, p. 60, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32008R0767, last accessed on 28 May 2021.

33 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L180, p. 1, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0603, last accessed on 28 May 2021.

34 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, OJ L135, p. 85, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0818&from=EN, last accessed on 28 May 2021; 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, OJ L135, p. 27, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0817&from=EN, last accessed on 28 May 2021.

35 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, OJ L119, p. 1 (GDPR), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, last accessed on 28 May 2021.

2. THE ASYLUM PROCEDURE

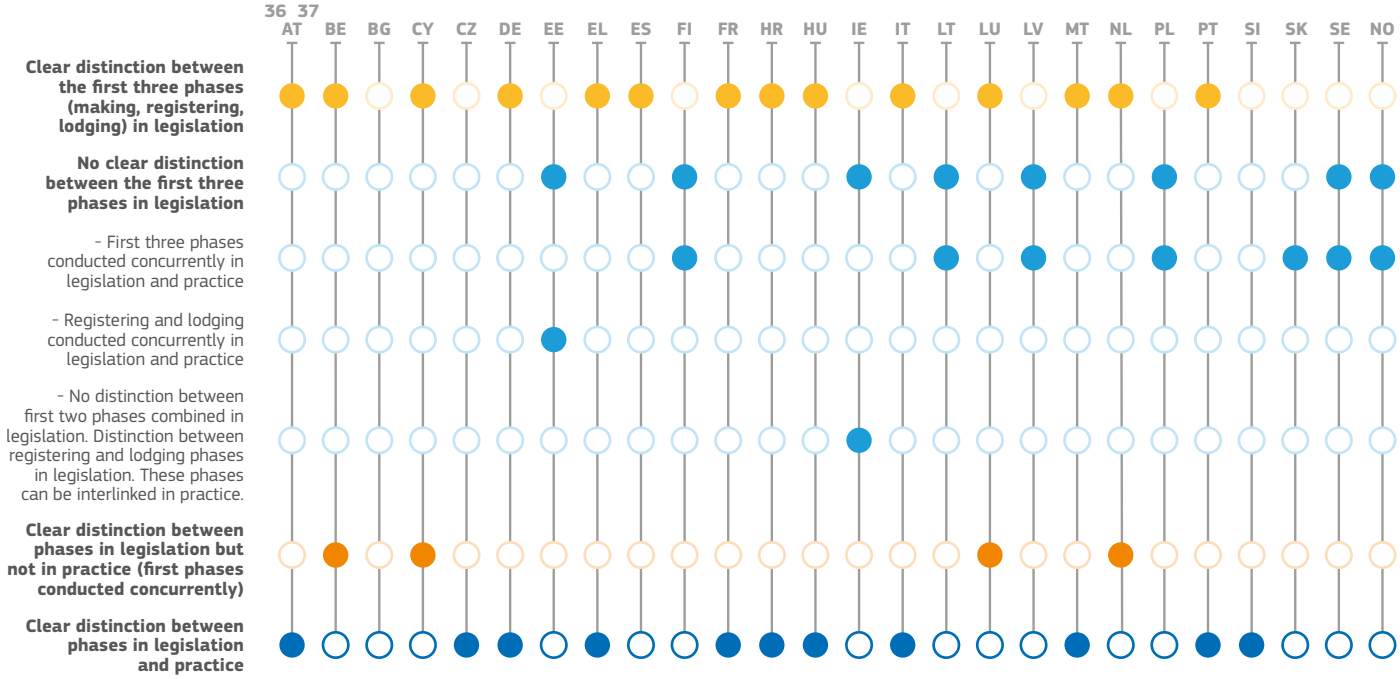
This section provides an overview of the different phases of the asylum procedure (see Section 1.2) in the Member States and Norway, from the point at which a person expresses their intention to apply for international protection, until a first-instance decision is adopted. Section 2.1 describes the phases of the asylum procedure, drawing a distinction between the different phases of the procedure in both legislation and practice. It then explores the use of channelling systems and timeframes between phases.

Section 2.2 describes the different authorities involved in the four phases of the asylum procedure. Section 2.3 explains how asylum applicants' data are collected during each phase of the asylum procedure, the authorities involved, methods of collection and storage tools used. Finally, section 2.4 provides an overview of how asylum applicants' data are managed in the different databases operated by the Member States and Norway.

2.1. OVERVIEW OF THE ASYLUM PROCEDURE

The EU Member States and Norway have adopted different approaches to the implementation of the phases of the asylum procedure, in both national law and in practice (Figure 2).

Figure 2. Overview of phases in Member States and Norway



Most Member States' national legislation clearly distinguishes between the first three phases of making, registering and lodging an application.[38] However, eight Member States and Norway do not provide a clear distinction in legislation,[39] with two or more phases conducted concurrently: making, registering and lodging an application for international

36 AT has no distinct registering phase.
37 Ibid.
38 AT, BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LU, MT, NL, PT, SI. AT has no separate registering phase.
39 EE, FI, IE, LT, LV, PL, SE, SK and NO.

protection constitute one administrative procedure and are therefore conducted simultaneously on the same day in six Member States and Norway.[40] Similarly, in Estonia, registering and lodging are conducted concurrently, while legislation in Ireland combines the making phase with the registering phase.

Twelve Member States clearly distinguish between the first three phases – making, registering and lodging – in both legislation and practice.[41] Of those that do not make a distinction in practice, Belgium, Cyprus, Luxembourg and the Netherlands nevertheless distinguish the three phases in legislation. In Belgium, registering the application takes place on the same day as making the application at the arrival centre, while lodging may take place a couple of days later at the Immigration Office. In Luxembourg, these three phases generally occur on the same day if the application is made to the Directorate of Immigration, while, in the Netherlands, the registering and lodging of a claim take place concurrently in a three-day process. When making the claim, the applicant is usually referred to the application centre, although it is possible that registration can take place immediately if the applicant is making the claim at one of the larger police stations or at a brigade (police station) of the Royal Netherlands Marechaussee. Similarly, in Cyprus, the registering and lodging phases are conducted concurrently in practice.

In many Member States and Norway, the means by which applicants enter the country (land, sea, air) has no bearing on how the application procedure is conducted.[42] However, five Member States reported that the entry route creates some practical differences in the distinction between asylum phases.[43] In Germany, a specific airport procedure takes place at five airports, meaning that the asylum procedure shall be conducted prior to the decision on entry if the asylum seeker can be accommodated on the airport premises during the procedure. However, the applicant needs to be granted entry if, among other reasons, the Federal Office for Migration and Refugees cannot decide on the asylum application within two days. In Ireland, a unit of the national police (the Garda National Immigration Bureau (GNIB)) registers persons who express an intention to make an application at the port of entry. The applicant is then referred to the International Protection Office, where the application is again registered before proceeding with the rest of the asylum procedure. Applicants who do not express an intention to make an application at the port of entry register their application at the International Protection Office. For Member States operating 'hotspots' (Italy and Greece), the making phase for entry by sea is carried out at the place of landing, in the hotspots, or in Reception and Identification Centres (RICs) with the support of interpreters and cultural mediators.

The national asylum legislation in most Member States and Norway[44] provides for an accelerated or prioritised procedure that allows authorities to process certain asylum applications more quickly, according to specific criteria.[45] This procedure can be applied to third-country nationals coming from a safe country of origin,[46] those refusing to have their fingerprints taken for Eurodac purposes,[47] those whose application is manifestly unfounded or contains false, inconsistent and contradictory information,[48] or those who have tried to evade border controls or for whom a return order has been issued.[49] Other Member States prioritise certain asylum applications in their national asylum law for certain categories of people, especially unaccompanied minors and other categories of vulnerable groups.[50] Some Member States implement admissibility procedures that consist of conducting a preliminary assessment on whether there are sufficient grounds to examine an asylum application.[51]

While some Member States' legislation provides no formal channelling system for specific cases, some applications are nonetheless prioritised or accelerated, such as subsequent applications, applications of unaccompanied minors or other vulnerable people, or applications of third-country nationals coming from a safe country of origin.[52] Since 2014, several Member States have provided for channelling systems for specific cases,[53] with most introducing multi-channel policies to make asylum procedures more efficient and accelerate the processing of applications for international protection.[54] In Estonia[55] and Lithuania, channelling procedures were introduced as part of their transposition of the recast Asylum Procedures Directive (Directive 2013/32/EU),[56] while, in 2015, Finland responded to the increasing numbers of applicants by automating the channelling of applications for international protection into different queues (see Box 1).

40 FI, LT, LV, PL, SE, SK and NO.
41 CY, CZ, DE, EL, ES, FR, HR, HU, IT, MT, PT, SI.
42 AT, CZ, EE, FI, HR, HU, IE, LT, LU, LV, NL, PL, SE and NO.
43 DE, FR, MT, PL, SK.
44 AT, BE, CY, DE, EE, ES, FI, FR, IE, IT, LT, LU, LV, MT, NL, PL, SE, SK and NO.
45 Recital 20 of the recast Asylum Procedures Directive (Directive 2013/32/EU) stipulates that 'Member States should be able to accelerate the examination procedure, in particular by introducing shorter, but reasonable, time limits for certain procedural steps, without prejudice to an adequate and complete examination being carried out and to the applicant's effective access to basic principles and guarantees provided for'. Article 31(8) of the Directive provides for the possible grounds for acceleration. While Ireland does not participate in the recast Asylum Procedures Directive (2013/32/EU), applicants can be prioritised pursuant to section 73 of the International Protection Act 2015.
46 AT, CY, FR, IT, LT, LU, NL, SK and NO.
47 LT, LU, SK.
48 AT, CY, FI, IT, LT, LU, MT, SE, SK.
49 IT.
50 EE, EL, IE, IT, LU, LV, NL.
51 FI, EL IE, IT, LT, LU, LV, NL, SE.
52 BE, DE, EE, IE, HR LU, PT.
53 AT, CY, DE, EE, FI, FR, IE, IT, LT, LU, NL. In Ireland, the prioritisation procedure relates to the scheduling of interviews.
54 AT, CY, DE, FR, IE, IT, NL, SE.
55 In EE, channelling refers to two options in legislation: either an accelerated procedure or prioritising an application.
56 Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection, OJ L 180, p. 60 (recast Asylum Procedures Directive), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex%3A32013L0032, last accessed on 28 May 2021.

Box 1 Automation in channelling procedures in Finland

Since 2015, asylum applications in Finland's Electronic Case Management System for Immigration (*Ulkomaalaisasiain sähköinen asiankäsittelyjärjestelmä* - UMA) are automatically channelled into different queues ('baskets') according to their urgency, based on keywords (or tags). The keywords may be created in two ways: either the UMA system generates keywords automatically on the basis of predefined rules (e.g. based on the applicant's date of birth, the system creates a keyword 'Asylum application, age group x'), or the user adds them manually (e.g. if the application has to be prioritised, it is added to the 'fast track' queue. Applications examined in Finland are further channelled to a location interview queue, based on the reception centre where the applicant resides. They are then divided into different 'baskets' on the basis of certain factors, including the urgency of the application, whether the case involves matters related to public order and security or exclusion, or the best interests of a child.

In accordance with Article 6(1) of the recast Asylum Procedures Directive, 10 Member States provide a time limit of three working days between making and registering an application.[57] For the lodging phase, however, Member States have adopted different time limits and timeframes, as Article 6(2) of the Directive merely states that the application must be lodged 'as soon as possible'. Austria does not apply explicit time limits for lodging an application,[58] for example, but the national legislation of Croatia and Hungary stipulate a time limit for lodging an application after the making phase of 15 and eight days, respectively.[59] Four Member States and Norway apply stricter rules,[60] according to which the entire procedure should be concluded in a shorter timeframe. In Croatia, Sweden and the Slovak Republic, the whole asylum procedure must not last longer than six months,[61] while in Norway, the aim is to conclude 70% of the asylum applications within 21 days.

Most Member States introduced these timeframes and/or time limits into their national legislation after 2014,[62] with some others amending their existing rules.[63] Assessing the average time lapse between making and lodging an application suggests that, in several Member States, the making, registering and lodging phases occur within the time limits established by their national laws.[64] In Cyprus and Norway, the average period from making to lodging an asylum application is longer than that provided by law. In Ireland, the International Protection Act 2015 does not provide for specified timeframes for the various phases of the international protection procedure.[65] Nine Member States have stipulated that the examining phase must be concluded in principle within six months of an application being lodged, as provided by Article 31(3) of the recast Asylum Procedures Directive.[66]

Overall, Member States' average period from making to lodging an asylum application within a normal procedure has not decreased significantly in recent years, with the exception of France and Italy (Table 1). In Italy, the making phase has always been carried out within 24 hours (maximum) upon disembarkation or interception on the territory, as part of the overall identification procedure. However, during periods of high influxes (2014-2017) the completion of the lodging phase saw Italy resorting to the extension of the time limit between the two phases fixed by law. France reported a decrease (from 18.2 days in 2017 to 5.8 days in 2019), following reform of the entire asylum procedure in 2015. That reform introduced several measures to reduce the time to register an asylum application (e.g. increase in the main authorities' personnel for lodging and examining applications), thus accelerating the lodging and examining phases. Croatia and Germany reported a slight increase in the average duration. In Germany, for example, the creation of arrival centres had an impact, as additional processes and actors were integrated into the procedures in order to decrease average processing periods in later stages. In Croatia, by contrast, the slight increase was due to the larger number of applicants and the extension of the duties of the competent authorities for lodging an application.

57 AT, BE, CZ (if the application is made to the Ministry of the Interior), EE, FR, HR (the deadlines apply only if the application has been made to the only competent authority – Ministry of the Interior), HU, IT, LU, NL (if the application is made to an immigration authority). In Italy, the law provides for the posisbility to extend the time limit up to 10 working days during periods of high influx.
58 The Federal Office for Immigration and Asylum is, however, required to order action without delay once it receives the information collected during initial questioning.
59 BE (within six months of an application being transferred to the asylum authority), CZ, EE, FI, FR, LU, MT, NL.
60 HR, LT, SE, SK and NO.
61 In Croatia, the law foresees that this time limit may be extended for nine more months according to the law (Article 40(3)).
62 BE, CY, EE, EL, FI, HR, HU, IT, LU, LT, LV, NL, SE.
63 CZ, EL, FR, IT, SK.
64 CZ, EE, FR, HR, LU, SK.
65 Ireland does not participate in the recast Asylum Procedures Directive.
66 BE, CZ, EE, ES, FI, FR, LU, MT, NL.

Table 1. Average days from making to lodging an asylum application

	2014	2015	2016	2017	2018	2019
CY			6-10	6-10	6-10	6-10
CZ	4-7	4-7	4-7	4-7	4-7	4-7
DE				9	13	14
EE	1	1	1	1	1	1
EL	1	1	1	1	1	1
HR	11	7	17	6	6	10
FR			8.8	18.2	8.3	5.8
IT	10	10	10	10	3	3
LU			1	1	1	1
LV			1-3	1-3	1-3	1-3
PL	1	1	1	1	1	1
PT	3-8	3-8	3-8	3-8	3-8	3-8
SI	1-3	1-3	1-5	1-5	3-7	3-7
SK	1	1	1	1	1	1

By contrast, several Member States experienced an increase in the period between lodging an application and the adoption of a first-instance decision until 2017-2018, followed by a downward trend between 2018 and 2019 (Table 2).[67] In Italy, the decrease in the average period between lodging an application and a first-instance decision was attributed to three factors: (i) reduction in the number of applications for international protection since 2017; (ii) additional personnel in the Territorial Asylum Commissions responsible for examining applications; (iii) an amendment to applicants' notification to appear before the examining Commission, which saw a substantial fall in the number of procedures pending and in the overall duration of the examination process. Similarly, in France and Luxembourg, hiring more personnel and a reorganisation of the internal structures of the authorities involved in lodging and examining an application shortened the processing time of asylum applications. Ireland's International Protection Act 2015 came into force on 31 December 2016; under the Act, the median overall processing time for international protection applications in 2018 was 19.7 months and in 2019 it was 17.5 months.[68]

Table 2. Average days from lodging until first-time decision in normal procedure[69] [70]

	2014	2015	2016	2017	2018	2019
AT	99	189	273	495	646	70[71]
BE	-	222	267	376	378	317
CY	365	365	365	365	365	365
CZ	176	188	182	181	163	129
DE	213	156	214	323	230	187
EE	100	125	67	37	57	73
ES	347	380	396	431	422	504[72]
FI	210	124	272	406	326	282
FR	263.27	261.8	220.49	220.53	176. 4	194.2
NL	118	185	150	111	172	103
LU	287.5	301	310.5	242	219	128
PL	200	118	86	221	247	152
SE	142	229	328	496	507	288
NO	102	130	253	338	204	218

67 AT, BE, CZ, DE, EL, FR, IT, LU, NL, PL, SE.

68 As Ireland does not participate in the recast Asylum Procedures Directive, the processing timeframes are not directly comparable. Prior to 31 December 2016, applications for refugee status and subsidiary protection were processed separately. Applications for refugee status were considered under the Refugee Act 1996 and applications for subsidiary protection under the Subsidiary Protection Regulations 2013 and 2015. The International Protection Act 2015 introduced the single application procedure from 31 December 2016.

69 In Italy, it is not possible to provide an estimate of the average days between the lodging phase and the first-instance decision, as the procedure is considered in its overall duration (from making to final decision following appeal). On average, the whole asylum procedure took around two and a half years between 2014-2017 and a maximum of one year in 2018 and 2019.

70 In 2017, Greece took less than 6 months from the lodging until a first-time decision was issued for most of the asylum applications (24 905), between 6 and 9 months for 4,136 applications, between 9 to 12 months for 3,237 applications and mor than 1 years for 4,052 applications. In 2018, Greece also took less than 6 months between lodging and asylum application and issuing a first-time decision for most applications (31,503) and more than 6 months for 27,290 applications. In 2019 the average time was between 20-180 days.

71 As of 2019, the duration of procedures was measured minus the procedures from the migration events of 2015/2016 (asylum applications until 1 June 2018).

72 The introduction of templates for decisions on the highest number of applications (Venezuelans and Colombians), as well as the decrease in applications due to the COVID-19 pandemic contributed to bringing down the average number of days for first-time decisions in the ordinary procedure to 293 in 2020. The average number of days in the border procedure is the same as the maximum set by law, as the consequence of not deciding and notifying the decision within the deadline (four days for applications and two days for re-examination requests) is the entry of that person into Spanish territory.

2.2. OVERVIEW OF AUTHORITIES INVOLVED IN THE ASYLUM PROCEDURE

The authorities involved in and responsible for the four phases of the asylum procedure – making, registering, lodging, and examining – vary significantly from one Member State to another. Nevertheless, it is possible to identify two main types of systems: a centralised system and a decentralised system. Several Member States have adopted a decentralised system, with more than one authority in charge of one or several phases of the asylum procedure[73] (e.g. in Portugal, five authorities are responsible for each phase). This is particularly true in the context of making an asylum application, with most Member States allowing three or more authorities to be involved.[74] In Slovenia, any public authority or self-governing local community (municipalities and provinces) can be involved when an application is made. A minority of Member States and Norway follow a more centralised system, whereby one authority is responsible for each phase of the asylum procedure – this is often the same authority throughout the entire procedure.[75] In Estonia, the Police and Border Guard Board (PBGB) is responsible for the entire asylum procedure, including the examination of the application. In the Netherlands, the national police and the Royal Marechaussee are responsible for the making, registering and lodging phase, but the examination of the application is solely the responsibility of the Immigration and Nationalisation Service (IND). In Norway, the National Police Immigration Service (NPIS) is responsible for the three concurrent phases in the asylum procedure.

Border police/guard and local police are involved in the making phase of the asylum application in almost all Member States.[76] In addition to the competent asylum authorities (e.g. local immigration offices, offices for refugees), several Member States also allow a first asylum application to be made from detention facilities and/or reception centres,[77] and Belgium allows directors of penitentiary institutions responsibility for making and lodging applications for international protection. Different EU and United Nations (UN) agencies provide support to Greece, Italy and Malta in the making phase. EASO supports the Greek, Maltese and Italian authorities by providing information on the asylum procedure to applicants for international protection. Italian authorities are also supported by the United Nations High Commissioner for Refugees (UNHCR) and the International Organization for Migration (IOM) for making applications for international protection at the hotspots.

In many Member States, the border police/guard is the primary authority responsible for registering and/or lodging applications.[78] In Finland, Italy, the Netherlands, Poland, Slovak Republic and Spain, the police authorities are competent for the first three phases of the asylum procedure, with the examination conducted by the Finnish Immigration Service, the Italian Territorial Asylum Commissions, the Dutch IND, the Head of the Office for Foreigners of Poland, and the Ministry of Interior of the Slovak Republic, respectively.[79] In 2015 and 2016, mobile teams coordinated by the Federal office for Migration and Refugees (BAMF) were deployed in Germany to facilitate registrations during a period of high influx of asylum seekers. The European Border and Coast Guard Agency (Frontex) supports Italian authorities with the registering phase in the hotspots, particularly identification procedures, querying EU information systems, and collecting data for statistical purposes. In the registering and lodging phases, Malta is supported by EASO officers, who also support Italian authorities in the lodging phase in selected police headquarters.

Finally, the examining phase is chiefly conducted by the competent ministry (e.g. Ministry of the Interior, Ministry of Justice, Ministry of Foreign Affairs),[80] the (local) immigration office,[81] or the office for refugees.[82] In Portugal and Norway, law enforcement authorities also play a role in examining asylum applications alongside other institutions. EU and international agencies support the national authorities in Cyprus, Greece, Italy and Malta in the examining phase - EASO officials work with Greek,[83] Maltese and Cypriot authorities in examining applications for international protection, while a UNHCR representative is part of the college of the Italian Territorial Asylum Commission responsible for examining applications for international protection.

73 AT, BE, CY, CZ, DE, FI, FR, HU, IE, LT, LU, LV, MT, NL, PT, SI.
74 BE, CY, CZ, FR, HU, LU, LV, MT, NL, PT, SI.
75 EE, EL, HR, IE, IT, PL, SE, SK and NO
76 Border police/border guard: BE, CY, CZ, DE, EE, ES, FI (Finnish Border Guard), FR (only for applications at the border), HR, HU, IE, IT, LU, LV, NL, PL, PT, SE, SI, SK. Local police: AT, CY, CZ, DE, EE, FI, HU, LU, LV, NL, PT, SE, SI and NO.
77 Detention facility: BE, CY, DE, EE, EL, FR, HR, HU, IE (Ireland does not operate immigrant detention facilities, but detainees in prison may express an intention to seek asylum and this is subsequently registered and lodged by the asylum authority (International Protection Office), LU, LV, MT, PT, SE, SI. Reception centre: CZ, DE, EL, ES, HR, HU, PT, SE, SI.
78 Registering: CY, EE (PBGB), ES, FR (only for asylum applications at the border), HR, IE (registering of applications made at port of entry), LV, NL, PL, PT, SI, SK; Lodging: EE, ES, LT, LV, NL, PL, PT, SK.
79 FI (border guard competent for registering/lodging asylum applications), IT, NL, PL, PT, SK.
80 CY, CZ, HR, IT, LU, LV, SI, SK and NO.
81 AT, FI, HU, LT, LV, MT, NL, PT, SE.
82 BE, DE, EL, ES, FR, IE, MT, PL.
83 In case of urgent need.

Table 3. Authorities involved in each phase of the asylum procedure

Type of authority	Phase			
	Making	**Registering**	**Lodging**	**Examining**
Border police/guard	BE, CY, CZ,[84] DE, EE,[85] ES, FI,[86] FR,[87] HR, HU, IE, IT, LU, LV, NL, PL, PT, SE, SI, SK	CY, EE, ES, FI,[88] FR,[89] HR, IE, LV, NL, PL, PT, SI, SK	CY, BE, EE, ES, FI,[90] LT, LV, NL, PL, PT, SK	PT
Local police	AT, CY, CZ, DE, EE, FI, HU, LU, LV, NL, PT, SE, SI,	CY, EE, FI, NL, PT, SI,	CY, EE, FI, NL, PT,	PT
(Branch) office for refugees	DE, EL, HU, IE,[91] MT, SI,	EL, IE, MT	DE, FR, IE	BE, DE, EL, ES, FR, IE, MT, PL
Ministries (Interior, Justice, etc.)	CY, CZ, FR,[92] HR, HU, IT, LU,[93] LV, SI	CZ, FR,[94] HR, IT, LU,[95] LV	CZ, HR, IT, LU,[96] LV, SI	CY, CZ, HR, IT, LU,[97] LV, SI, SK,
Local citizens' office/ mayor of city/town	HU, SI			
(Local) immigration office	AT, BE, DE, EE, FI, FR, HU, IT,[98] MT, PT, SE, SI	AT, BE, EE, FI, FR, HU, IT,[99] MT, PT, SE and NO[100]	AT, BE, EE, FI, HU, IT,[101] LT, MT, PT, SE and NO[102]	AT, EE, FI, HU, LT, MT, NL, PT, SE and NO[103]
(Shared) accommodation for refugees	DE, HR, HU	HR	HR	
EU agency	EL (EASO), IT (EASO), MT (EASO)	EL (EASO), IT (Frontex), MT (EASO)	EL (EASO), IT (EASO), MT (EASO)	CY (EASO), EL (EASO), MT (EASO)
International organisation	IT (UNHCR, IOM)			IT (UNHCR)
Detention facility	BE, CY, DE, EE, EL, ES, FR, HR, HU, LU, LV, MT, PT, SE, SI,	HR, MT, PT, SE	MT, PT, SE	MT, PT
Reception centre	DE, EL, ES, FR,[104] HR, HU, PT, SE, SI,	DE, HR, PT, SE	HR, PT	PT
Other				
Penitentiary institution	BE (director), IE, LU		BE (director)	
Control service airport	LU			
Mobile teams (2015 – 2016)	DE	DE		

84 In CZ, there is no border police/guard, but the 'Foreign Police' does not solely perform border security and its scope of activities is much wider than it is attributed to border police.
85 In Estonia, the PBGB is responsible for all phases.
86 Border guard.
87 Only for asylum applications at the border.
88 Border guard.
89 Only for asylum applications at the border.
90 Border guard.
91 The International Protection Office is an office of the Department of Justice.
92 In FR, the Ministry of the Interior is represented by an association at an Initial Reception Centre for Asylum Seekers (SPADA).
93 Ministry of Foreign and European Affairs, Directorate of Immigration.
94 In FR, the Ministry of the Interior is represented by the agents of the prefecture and the OFII at the single desk for asylum seekers (GUDA).
95 Ministry of Foreign and European Affairs, Directorate of Immigration.
96 Ibid.
97 Ibid.
98 Refers to the local immigration office included in the police headquarters.
99 Ibid.
100 In Norway, the NPIS is responsible for the three concurrent in the asylum procedure.
101 Refers to the local immigration office included in the police headquarters.
102 In Norway, the NPIS is responsible for the three concurrent phases in the asylum procedure.
103 Ibid.
104 The SPADA does not accommodate asylum seekers.

2.3. DATA COLLECTED DURING THE ASYLUM PROCEDURE

This section provides an overview of the data collected at registering/self-registering, lodging and examining phases of the asylum procedure in the Member States and Norway. It focuses on the different types of data gathered and the authorities responsible in the registering, lodging and examining phases. This is followed by an overview of the methods and storage means used. Finally, it draws together some good practices in data collection, as identified by the Member States. With regard to data collection (see section 2.3.1), the Member States and Norway only reported on data collected and/or re-collected in each of the phases of the asylum procedure and not on data reused in those phases.

2.3.1. Data collected in the registering, lodging and examining phases

The type of data collected and the phases of the asylum procedure in which they are collected vary between the Member States and Norway (see Annex 2). All Member States and Norway collect data on applicants' current and/or birth names during the registering phase of the asylum procedure, but several Member States also collect this information in subsequent phases.[105] While most Member States and Norway collect the pen name (alias) of the asylum applicant,[106] few collect their religious name.[107] Ireland uses the category 'other names'. Data such as date of birth and citizenship(s) are also collected at the earliest possible stage by all Member States and Norway, with several collecting/re-collecting it in the lodging phase.[108]

All Member States collect biometric data (photo and fingerprints) during the registering and/or lodging phases, except for the Czech Republic, which collects fingerprints during the making phase and the photo during the lodging stage.[109] Austria collects an additional photo in the examining phase, while Finland may collect it in this phase if it was not collected earlier. Greece takes an iris scan during the registering phase, although few other Member States record applicants' eye colour or height.[110]

In addition to the traditional contact details (e.g. phone number, email address) collected by all Member States, Finland, the Netherlands and Norway also collect applicants' social media profile(s). Information on family members is collected by all Member States,[111] but not necessarily in the registering phase. For example, a number of Member States collect information on the names of family members in the lodging or examining phases. [112]

Information on the health status of applicants for international protection is collected by all Member States, but in some cases, this information is collected after the registering phase.[113] For example, in Austria, Luxembourg, the Netherlands[114] and the Slovak Republic,[115] applicants' health status is checked only during the examining phase. While most Member States and Norway collect information on education, that collection mostly takes place during the examining phase,[116] with one-third of Member States collecting information on education during the registering phase,[117] and a few during the lodging phase.[118]

Information on the reasons for fleeing is first collected in the registering phase in 10 Member States[119] and in the lodging phase in 12 others.[120] In Norway, this information is collected only in the examining phase. Although the Netherlands asks for it during the registering or lodging phase for proper identification, the reasons for fleeing are usually only registered during the examining phase.

Criminal records are requested in most Member States and Norway, and such information is generally gathered when the applicant registers their application.[121]

Data on vulnerabilities (e.g. whether the applicant is a pregnant woman, a disabled person, a single parent with a child, suffering from a mental disorder, or a victim of human trafficking or torture) are collected and re-collected throughout the asylum procedure. Most Member States and Norway collect such data during the registering phase,[122] but 12 others collect/re-collect these data in subsequent phases.[123]

A trend in frontloading the collection of some elements of asylum seekers' data is evident for several categories of personal data, including name, biometrics, place of birth and supporting documents (e.g. passport and travel documents). Most Member States and Norway generally collect the applicant's personal data during the registering and lodging phases.[124]

105 AT, CY, CZ, ES, HR, HU, FR, IT, LV, PT, SI, SE, SK and NO.
106 AT, BE, CZ (not mandatory), DE, EE, EL, ES, FI, FR, HR, HU, IT, LU, LV, NL, PT, SE, SI, SK and NO.
107 DE (not mandatory), EL, ES, HU, IT (Italian forms do not include a specific field for 'religious name', but the rationale of the registering and lodging phases is to collect all information provided by the applicant), PL, PT SK.
108 BE, CY, CZ, FR, HR, HU, IT, LT, LV, PT, SE, SI.
109 Photo: AT, BE, CY, CZ, DE, EE, EL, FI, FR HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, SE, SI, SK and NO.
Fingerprints: AT, BE, CY, DE, EE, EL, FI, FR HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, SE, SI, SK and NO.
110 Eye colour: AT, BE (only for unaccompanied minors), DE, EL, FI, IT, LV, PL. Height: AT, BE, DE, EL, FI, IT, LV, MT, PL, SE.
111 AT (collected on a voluntary basis), BE, CY, CZ, DE, HR, HU, EE, EL, ES, FI, FR, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SE, SK.
112 Registering: CY, DE, EE, EL, FR, HR, LV, NL (self-registration), SE. Lodging: BE, CZ, ES, FR, HR, IE, IT, LT, MT, NL, PT, SI. Examining: AT, FR, HR, LU, NL, SK.
113 Registering: BE, CY, DE, HR, EE, EL, HR, HU, IT (if poor health or vulnerabilities (e.g. pregnancy) are evident at the making or the registering phase), FR, LV, SE. Lodging: BE, CZ, HR, EE, HU, FR, IE, IT, LT, LV, MT, PL, PT, SI, SE, NO. Examining: AT, BE, CZ, HR, EE, FI, HU, FR, IT, LU, NL, SK, NO. ES: Applicant is not asked any specific questions about their health at any stage, without prejudice to the applicant mentioning them as a reason for their application, the official taking a statement, or the instructor asking for evidence of vulnerability of the applicant.
114 The health check in the examining phase is done before the actual start of this phase to determine if the applicant can be interviewed. In the registering phase, the applicant is checked for tuberculosis and in the reception centres the applicant has access to medical care.
115 With the exception of asylum applications lodged in the detention centre, when health status is checked in the registering and lodging phase.
116 CY, FI, FR, HR, HU, IE, LU, SK and NO. In Ireland, this information is collected during the examining phase but can be collected earlier if volunteered by the applicant.
117 AT, DE, EE, EL, HR, LV, NL, PL, SE.
118 BE, ES, FR, HR, IT, LT.
119 AT, EE, EL, FI, IE, LU, LV, NL, PL, SK.
120 BE, CY, CZ, DE, ES, FR, HR, IT, LT, MT, NL, SI. In IT, this information is collected during the making phase and re-collected in the lodging phase.
121 During registering: DE, EE, EL, FR, IT, LT, LV, NL, PL, SK and NO; During lodging: HR, HU, FR, IT, NL, PL, PT, SK, SE and NO; During examining: ES, FR, HR, IT, LV, MT, PT, SI.
122 BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, LU, LV, NL, PL, SE, SK and NO.
123 AT, BE, CZ (except data on unaccompanied minors, which are collected in the registering phase), FR (data collected in the registering, lodging and examining phases), HR, IE (can also be collected at registering if volunteered by applicant, or for unaccompanied minor applicants), IT (vulnerabilities are collected when the asylum seeker is identified and are then ascertained in the lodging stage), LU (except data on unaccompanied minors, which are collected in the registering phase), LT, MT, PT, SI.
124 BE, CZ, DE, EE, EL, ES, FI, FR, IE, LT, LU, LV, MT, NL, SE, SI, SK and NO.

Box 2 Good practices and challenges in frontloading information collected

The frontloading of data collection is considered good practice by some Member States[125] for reasons including: it allows applicants' necessary information to be obtained in the early phase of the asylum procedure and transmitted together to the authorities responsible for the subsequent phases;[126] it saves on administrative capacity,[127] or invests administrative capacity at an earlier stage to save it at a later one;[128] it can allow other competent institutions immediate access to the data;[129] and it allows for the categorisation and prioritisation of certain applications.[130]
Cyprus, Croatia, Germany and Norway also frontload information collected by authorities not directly connected to the asylum procedure. Cyprus extracts certain data from the Civil Registry and Migration Department, including previous employment and residence status. This is considered good practice, as it facilitates an encompassing image of the claim, including reception and procedural needs of the applicant. In Germany, an employment agency can access data on education, profession, training and language skills, as well as record specific data on previous professional experience and qualification. In Croatia, competent health authorities collect information on applicants' health status before lodging the asylum application. In addition, organisational units within the Ministry of the Interior (not directly connected to the international protection procedure) collect data on certain forms of security issues, such as criminal records and offences. These are considered good practices, as they provide the information necessary to organise quality reception and accommodation for applicants for international protection, as well as adjustments for security measures.

All but four Member States[131] repeat the collection of some categories of applicants' data across the different phases in the asylum process (registering, lodging and examining).[132] The types of data that are collected several times during the asylum procedure include: reason(s) for fleeing,[133] citizenship,[134] place and date of birth,[135] and vulnerabilities.[136] In Greece, by contrast, all information is gathered only during the registering phase. In Germany, most data are gathered during the registering phase, with few exceptions of data gathered at an earlier or later stage. Data are only added if new information is gathered or data collected in an earlier stage were incorrect, incomplete or of insufficient quality.

2.3.2. Authorities responsible for data collection during the registering, lodging, and examining procedures

Frontloading the collection of applicants' information results in an increased amount of data collected by the authorities responsible for registering and lodging applications. Border police/border guards and local police are the main authorities involved in these phases in most Member States and, as such, they collect the majority of data in the registering and lodging phases of the procedure.[137] In Ireland, data collected at the registering phase can be collected by police at the port of entry and by the office responsible for examining protection applications.[138] This office is solely responsible for data collected at the lodging phase.

Similarly, as (local) immigration offices and ministries are the main authorities involved in examining an application in most Member States, they are also the main authorities involved in gathering applicants' data in that phase.[139] In some Member States and Norway, reception facilities chiefly collect data on health attendance, education and vulnerabilities, used during the examining phase,[140] or are the main authorities involved in gathering applicants' data.[141]The Netherlands and Norway reported contributions from the police to information collection across a range of data categories used during the examining phase. However, in several Member States, a single authority gathers applicants' data throughout the entire asylum application.[142] This results in less repetition of data collection at the different phases in Estonia and Greece, but not in Hungary and Poland, where applicants' data are still gathered in each of the different phases. Finally, it is worth noting that Croatia has three authorities under the Ministry of Interior involved in data collection at each phase of the asylum procedure.

2.3.3. Methods used to collect data during the asylum procedure

During the asylum procedure, applicants for international protection provide data to support their application. This information is mainly collected through oral interviews (face-to-face) and questionnaires completed by the applicant.[143] Electronic tools (cameras and specific fingerprint equipment) are used to collect biometric data. The analysis of documents is less widespread and is mainly used to gather information on the date of birth, citizenship, country of origin and country of birth of asylum applicants.[144] Greece, the Netherlands and Norway rely on online self-registration to collect almost all applicants' data. Germany

125 DE, EE, EL, FI, LV, NL.
126 DE, EE, LV, NL.
127 LV.
128 DE
129 DE, LV, NL.
130 EL, FI.
131 EL, MT, LT, LV.
132 AT, BE, CY, CZ, DE, EE, ES, FI, FR, HR, HU, IE, IT, LU, NL, PL, PT, SE, SI, SK and NO.
133 BE, CY, CZ, DE, EE, FI, FR, HR, IE, IT, LU, LT, MT, NL (normally only in examining phase, but for identification purposes, sometimes in registering phase), PL, SI, SK.
134 AT, CY, CZ, FR, HR. HU, IT, LT, PT, SI, SK and NO.
135 AT, CY, CZ (requested only in the registering phase, but it is also registered in the lodging phase if mentioned by the applicant), FI, FR, HR. HU, IT, LT, PT, SI, SK and NO.
136 AT (only unaccompanied refugees), BE, CY, EE, ES, FR, FI, HR, HU, IE, IT, LT, NL, PL, PT, SE, SK and NO.
137 AT, EE, ES, FI (border guard), HR, LT, LV, NL, PL, PT, SI, SK.
138 International Protection Office.
139 Local immigration office: AT, EE, CY, FI, HU, IT (immigration offices embedded in the national police headquarters, Questure), LT, NL, SE. Ministry: HR, IT, LU, SI, SK and NO.
140 Health attendance: FI, HR. Education: DE, HR, NL and NO. Vulnerabilities: DE, HR, NL.
141 DE.
142 EE, EL, ES, HR, HU, IT (different departments within the Ministry of the Interior), LU (except biometric data collected by the judicial police), PL, SE.
143 Oral interview: AT, BE, CY, EE, EL, HU, FR, HR, IE, IT, LV, MT, NL, PL, PT, SI, SK, SE and NO. Questionnaires: AT, CY, CZ, EE, EL, FR, IE, HU, LU, LV, MT, NL, PT, SE, NO.
144 CY, CZ, DE, EE, ES, FR, FI, HR, IT, LT, LU, NL, PT, SK, SE and NO.

uses document analysis for a wide range of data categories where supporting documents are available (birth certificate, passport, medical certificate, school certificates, etc.), with several other Member States also using new methods and technologies to collect data on asylum applicants.[145] In some cases, these rely on the use of open sources (e.g. social media) to retrieve different types of data, ranging from biographical information to vulnerabilities, previous education and credibility of the application.[146] Italy and Norway may consult these sources to retrieve any data collected in different phases of the procedure. Finland, Lithuania and Portugal use open sources to collect certain types of data: Finland only uses open sources to retrieve aliases, Lithuania to discover applicants' reasons for fleeing, and Portugal to collect information on certain vulnerabilities, reasons for not wanting to return to the competent Member State, information on the route taken and applicants' religious affiliations. Similarly, Germany and Norway analyse mobile devices' content to gather and evaluate information on the applicant. For example, German authorities use this method to verify identity and citizenship. Mobile devices are also used by Portugal to collect applicants' aliases, and by France to collect information on close relatives in other Member States. Finally, it is worth highlighting that France and Greece use automated processes or AI to gather certain types of data (i.e. current name, alias and sex in France, biometric data in Greece, and criminal record in the Netherlands).

2.4. OVERVIEW OF DATA MANAGEMENT IN THE ASYLUM PROCEDURE

Data collected during the asylum procedure are stored in various ways across the Member States and Norway using three different methods: electronic files, databases, and paper files. Databases appear to be the most frequently used, especially when registering and lodging an application.[147] Some of these data are stored in the national databases of the different authorities involved in the asylum procedure,[148] such as the office for examining protection applications, the immigration service,[149] reception centres,[150] or border and local police registers.[151] Nevertheless, while some Member States rely on databases and electronic files for the most part,[152] others also use paper files[153] (in some cases exclusively) for certain type of data[154] (information on family members in another Member State,[155] health status,[156] and certain vulnerabilities[157]).

Box 3 Estonia – Register of Granting International Protection (RAKS)

Estonia uses a national centralised database to support all phases of the asylum procedure – the Register of Granting International Protection (*Riiklik rahvusvahelise kaitse andmise register* – RAKS). RAKS collects information on applicants for international protection, applicants for a residence permit on the basis of temporary protection, refugees, persons eligible for subsidiary protection, persons eligible for temporary protection, and family members of beneficiaries of international protection.

The aim is to process the personal data of persons who have submitted an application for international protection, together with the data relating to these proceedings. RAKS is fully managed by the PBGB, as the only authority competent for the entire asylum procedure. The authorised database processor is the Technology and Development Centre of the Ministry of the Interior.

Most databases (or the data they contain) may be accessed or shared with a variety of authorities in the course of the asylum procedure.[158] In most cases, the institutions and organisations authorised to access these databases are those involved in the asylum procedure. However, several Member States and Norway allow institutions outside the asylum procedure to access either specific databases or specific categories of data (e.g. through transmission or sharing by another authority).[159] In Luxembourg, the Ministry of Health can access the asylum services databases to identify applicants who must undergo a medical check. Similarly, national labour authorities and employment agencies may access specific data in Germany, Luxembourg and the Netherlands.[160] In certain instances, other authorities (e.g. military authorities, intelligence services) have access to asylum services databases or specific categories of data contained in these databases for purposes outside asylum procedures, such as security reasons.[161] The Swedish Police Authority and the Swedish Security Service have access to the Central Database for Aliens Affairs in order to

145 BE, DE, EL, FI, FR, LT, NL, PT and NO.
146 BE, FI, IT, LT, PT, SE and NO.
147 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.
148 BE, CZ, DE, ES, FI, HR, IE, LT, LV, NL, SE, SI.
149 In Ireland, data relevant to the asylum procedure are stored on the case management database of the International Protection Office. In addition, certain limited identifying data (e.g. name and contact details) are stored on the general case management system of the Immigration Service Delivery of the Department of Justice. The case number is generated by the Immigration Service system.
150 CZ, DE, FI, HR, NL.
151 CZ, ES, FI, HR LT, NL, SE, SI.
152 AT, BE, DE, ES, FI, NL, PT, SI, SE and NO.
153 CY, CZ, EE, EL, FR, HR, HU, IE, IT, LU, LT, LV, MT, PL, SK.
154 CY, CZ, HR, HU, LT, LU, PL, SK.
155 CY, CZ, LT, LU, SK.
156 CZ, HR, LT, LU, SK.
157 CY, CZ, HR, LT, LU, SK.
158 DE, EE, ES, FI, IE, LU, NL (through the BVV database), SE, SK.
159 CZ, DE, LU, IE, NL, SE, SK.
160 In the Netherlands, only the Inspectorate of Social Affairs and Employment has access to the BVV database, as it is involved in upholding the labour laws, including those for third-country nationals or trafficking in human beings in labour exploitation.
161 DE, SE, SK and NO.

prevent and act on criminal charges. Similarly, in the Slovak Republic, the Military Intelligence and the Slovak Information Service have access to the national migration and asylum database (Information System for Migration and International Protection - IS MIGRA) for evaluating potential security threats.

Apart from the data that Member States share through EU information systems, three Member States reported sharing data contained in national databases (e.g. personal data and border crossing information) with other Member States in certain circumstances.[162]

Box 4 Good practice in the Netherlands: connecting all authorities[163]

In order to secure the uniform use of personal data by all authorities involved in the asylum procedure, the Dutch authorities use the Central Shared Database with Basic Information on Applicants (*Basisvoorziening Vreemdelingen*, (BVV). Once a third-country national is identified and registered, all connected authorities make use of the (frontloaded) data collected. Adding/adapting these data is strictly regulated.
Asylum applicants are first registered in the BVV, with a connection made with the Municipal Personal Records Database (Basisregistratie Personen, BRP) at the end of the registering phase. Other third-country nationals might be registered first in the BRP and that information frontloaded automatically into the BVV.

162 FI, HU, NL.
163 According to interviews with the police, the Royal Marechaussee and the Dutch Council for Refugees, this is considered good practice because it avoids confusion between different personal data for one person.

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

This section starts by exploring the process of making an asylum application to an authority that is not competent to register the application, in those Member States that differentiate between 'making an application' and 'registering an application' (section 3.1). It then provides an overview of several aspects related to data management in the subsequent registering, lodging and examining phases (sections 3.2 – 3.4), looking first at the databases against which asylum applicants' data are cross-checked and then at the issues encountered during that cross-checking process. Other aspects discussed for each of the phases are the type and means by which information on rights as data subjects is provided to asylum applicants, and whether training is offered to national authorities responsible for data management in the Member States and Norway. The self-registration procedures set up in two Member States and Norway are also described.

Table 4 provides an overview of the types of databases cross-checked by Member States and Norway in the different phases of the asylum procedure.

Table 4. 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

164 In NL, the registering and lodging phases are combined (see section 3.3).

3.1. MAKING AN APPLICATION FOR INTERNATIONAL PROTECTION TO AN AUTHORITY NOT COMPETENT TO REGISTER THE APPLICATION

Third-country nationals making a claim for international protection do not always do so before the authorities that are competent to register the application. In most Member States, authorities that are not competent to register applications for international protection but are involved in the making phase provide applicants with information on the registration process and/or direct the person to the competent authority.[165] In Cyprus, the national authorities, non-governmental organisations (NGOs) and EU agencies provide written information (leaflets) and operate info-points. In Germany, if the application is made with the Federal Police, it refers to the 'Information on police data processing by the Federal Police' as well as the 'Information on non-police data processing by the Federal Police', which can be accessed online.

Some Member States have specific measures to provide information on registering an application to third-country nationals in detention facilities.[166] In Luxembourg, if a person expresses their intention to make an application, a caseworker from the Directorate of Immigration will visit the detention centre and collect all the data needed to register and lodge the application for international protection. Similarly in Latvia, public authorities contact or forward the application to the State Border Guard, so that it can carry out activities in accordance with the Asylum Law.

In Luxembourg, national law foresees that the ministry responsible provides personnel of non-competent authorities with the training necessary to fulfil their duties, as well as information on how to adequately inform applicants about where and how they can make their application for international protection. By contrast, Austria reported that non-competent authorities inform the competent authorities directly and usually refer applicants to the police or the Federal Office for Immigration and Asylum. However, there seems to be no systematic procedure for these referrals, which seem to happen in isolated cases, depending on the experience of the individual public employee involved. In Austria, Croatia, Germany and Slovenia, non-competent authorities are obliged to inform and report the case to the competent authority or (in some circumstances) the police/security service. In Italy, non-competent authorities must report the case to the competent police headquarters and/or inform the applicant that they must go to the police headquarters to apply for international protection.

Several Member States reported that where authorities lack the competence to register applications for international protection, they refrain from collecting data from applicants in this phase.[167] By contrast, in seven Member States,[168] some non-competent authorities involved in making the application do collect data on asylum applicants. The most commonly collected data are: current name and date of birth,[169] citizenship,[170] fingerprints,[171] and information on the identity of the person.[172] The Czech Republic and Germany collect information on unaccompanied minors applying for asylum, and German and Maltese non-competent authorities collect information on spoken languages and gender. In Germany, non-competent authorities collect fingerprints and facial images, in addition to personal information, during the making phase. These are collected through PIK stations (see Box 5) and are also printed on the certificate of registration as an asylum seeker. Similarly in Italy, fingerprints may be collected during the making phase, although this is not done systematically. In the Czech Republic, certain other categories of data can also be collected with the applicants' permission (e.g. alias, citizenship or place of birth).

Box 5 PIK stations in Germany

The 'PIK' is the so-called personalisation infrastructure component, while the 'PIK station' is a hardware and software solution for recording the PIK. The PIK station consists of a fingerprint scanner, a camera for taking facial images, a passport scanner for reading personal documents, software for data storage, and a printer (e.g. for issuing proof of arrival). The PIK station enables automated storage of personal data in the Migration Asylum Reintegration System (MARiS) and in the Central Register of Foreigners (AZR). At the same time, fingerprint data are stored in police databases, allowing an automatic security cross-check at the earliest possible date.

Finally, all Member States that reported that authorities who are not competent to register an asylum application collect data at the making stage also reported transferring this information onwards to the competent authorities.[173]

165 AT, CZ, CY, DE, EE, FR, HR, HU, HU, IE, IT, LU, LV, NL, PT, SE.
166 FR, IE (Ireland does not operate immigration detention facilities. In prisons, the Prison Governor contacts the International Protection Office when a person expresses an intention to seek asylum), LU, LV.
167 AT, EE, FI, HR, LU, LV, NL, PT, SE, SI, SK.
168 CZ, DE, FR, HU, IE, IT, MT.
169 Current name and date of birth: CZ, DE, HU, MT.
170 DE, HU, MT.
171 DE, IT.
172 CZ, DE, EL.
173 CZ, DE, FR, HU, IE, IT, MT.

3.2. REGISTERING AN APPLICATION FOR INTERNATIONAL PROTECTION[174]

During the process of registering an application, several Member States reported cross-checking applicants' data against national,[175] European[176] and international databases (Table 4).[177] For European databases, several Member States systematically cross-check data on asylum applicants against the VIS[178] and SIS[179] at this stage.[180] Additionally, half of the Member States also check fingerprints against Eurodac during the registering phase. In Belgium, Italy and Germany, the fingerprints of applicants for international protection are cross-checked with the national fingerprints database to determine if the applicant is already known to the national authorities due to (a) previous applications, and/or (b) previous illegal stay in the countries. As such, the cross-checking also allows for detection of identity fraud. Similarly, the Czech Republic cross-checks data with national databases, searching for previous applications or residence permits, primarily to acquire additional information that is used later in the asylum process. Information on national and international arrest warrants is also cross-checked against the Czech national fingerprints database and Interpol, respectively.

Three Member States reported encountering issues when cross-checking data collected in the registering phase.[181] In the Czech Republic and Malta, those issues related to lack of information or the provision of false information. Italy highlighted issues related to the transliteration of applicants' names due to the different rules adopted by Member States, as well as the need for more information to be input into Eurodac and the insufficient speed of data processing systems.

Box 6 Self-registration procedures

In Greece, the Netherlands and Norway, self-registration terminals or booths are located within the premises of administrations for applicants to self-register.[182] These were implemented in Greece in 2020, in the Netherlands in 2015-2016, and in Norway in 2018. All three self-registration systems are based on a website and asylum applicants are given information before using the system. In Greece, information is given by the first Reception and Identification Service (RIS).

In the Netherlands, an employee from the IND opens the digital application form, installs the correct language, and guides the asylum seeker (in person) if they have any questions. In Greece, in cases where pre-registration has not been fully completed by competent authorities, applicants are required to complete the registration procedure through the self-registration website. In the Netherlands, applicants may choose between the self-registration procedure and an application in writing. In Norway, it is available for those that are capable of using it - applicants who are illiterate or who do not speak one of the available languages are exempt and may use the normal procedure. The self-registration platforms are available in two languages in Greece,[183] in 17 languages in the Netherlands,[184] and 16 in Norway.[185]

At the registering stage, 12 Member States provide applicants with a privacy note containing information about their personal data being collected (Table 5).[186] In most cases, the privacy note is provided by the public authorities, for example, the Ministry of the Interior in the Czech Republic, Croatia (Reception or Detention Centres), Italy, Hungary (National Directorate-General for Aliens Policing) and Portugal (Foreigners and Borders Service), or the border police in Croatia and Hungary. Those 12 Member States provide this information in writing,[187] and most of them offer translation services (usually provided by public authorities, such as the Ministry of the Interior in the Czech Republic, Croatia and Italy).[188] Apart from the information provided in writing, 10 Member States also provide information verbally,[189] with Estonia, Greece, Italy, the Netherlands and Norway also providing it digitally. Interpretation and translation services are offered in most cases. In Greece, staff of NGOs and other international organisations support the asylum service in information provision, and in Italy, the UNHCR supports the Ministry of Interior with the preparation of the privacy notice.

Six Member States provide specific training or guidance for the staff responsible for data management with respect to information collected in the registering phase.[190] For example, in Italy, the state police and EASO have provided training for more than 500 officers.

174 In some Member States (CY, EE, FI, LT, LU, LV, NL, PL, SE, SK) and NO, the phases of registering and lodging are conducted concurrently (see section 2.1). Information on those Member States is included in section 3.3.
175 BE, CY, CZ, DE, EE, FR, HR, IE, IT, MT, NL, SE, SI. In NL, the registering and lodging phases are combined (see section 3.3).
176 BE, CY, CZ, DE, EE, EL, FR, HR, IE, IT, MT, NL, SE.
177 CY, CZ, HR, PT, SI.
178 BE, CZ, DE, EE, EL, IT, MT, NL, PT, SE.
179 BE, CZ, DE, EE, EL, HR, IT, MT, NL, PT, SE, SI.
180 Ireland does not participate in VIS. Ireland is not part of the Schengen area but participates in some non-border related aspects of SIS II, in accordance with Council Decision 2002/192/EC and Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of certain provisions of the Schengen acquis in Ireland. As Croatia is not part of the Schengen Area, it only has access to the Croatian VIS.
181 CZ, IT, MT.
182 EASO, 'Practical recommendations on conducting remote/online registration (lodging)', June 2020, https://easo.europa.eu/sites/default/files/easo-practical-recommendations-conducting-remote-online-registration-lodging-EN.pdf, last accessed on 10 June 2021.
183 English and Greek.
184 Albanian, Amharic, Arabic, Bosnian, Croatian, Dari, English, Farsi, French, Pashtun, Punjabi, Russian, Serbian, Spanish, Tigrinya, Turkish and Urdu.
185 Norwegian, English, French, Oromo, Turkish, Albanian, Arabic, Dari, Kurmanji, Pashto, Persian, Russian, Somali, Sorani, Tigrinia and Spanish.
186 CZ, DE, EE, EL, ES, FR, HR, HU, IT, NL, PT, SE.
187 CZ, DE, EE, EL, ES, FR, HR, HU, IT, NL, PT, SE.
188 CZ, DE, EE, EL, HR, HU, IT, NL, PT.
189 CZ, DE, EE, EL, FR, HU, IE, IT, NL, PT.
190 DE, EL, IE, IT, PT, SI.

3.3. LODGING AN APPLICATION

Most Member States and Norway cross-check the information collected during the lodging phase against national,[191] European,[192] and international[193] databases (Table 4). Some examples of national databases cross-checked at this stage include national population registers,[194] or registers for wanted persons.[195] Criminal records databases are consulted in Estonia, while Latvia consults the national Register of Returned Foreigners and Entry Bans. In Luxembourg, the National Intelligence Service consults its internal database, which contains information on counter-terrorism, counter-espionage, counter-proliferation, organised crime and cyber activities.

For European databases, most Member States and Norway conduct systematic cross-checking against VIS[196] and SIS[197] during the lodging phase, while 10 Member States[198] also cross-check fingerprints against Eurodac. Additionally, four Member States and Norway reported consulting the Interpol SLTD database in this phase.[199]

A number of Member States reported encountering issues in cross-checking data during this phase.[200] The most common problems include the interoperability of EU databases,[201] the accuracy of the data provided,[202] applicants' lack of travel documents,[203] and transliteration of applicants' name (especially in non-Latin alphabets).[204] Austria highlighted that the lack of automated processing and data entry issues hinder the interoperability of EU databases. The Netherlands pointed to the increased workload when information comes from the predecessor of the BVV database or where deviations are identified in the data retrieved from different databases. Four Member States noted the issue of inconsistencies between the data provided by applicants, or false data.[205]

Most Member States and Norway provide applicants with a processing/privacy notice during the lodging phase (Table 5).[206] This information is typically provided by the public authorities responsible for migration and/or international protection,[207] border guard/police,[208] reception centres,[209] and NGO staff.[210] Malta is in the process of establishing a system to ensure that applicants are provided with information on their rights as data subjects, as required by the GDPR. Similarly, a processing/privacy notice will soon be put in place in Luxembourg.

In this phase, information on data processing is provided in writing in 18 Member States and Norway.[211] Austria, Belgium, Germany and Portugal distribute leaflets, for example. Virtually all Member States providing the information in writing make translations available to applicants.[212] In Estonia, a processing notice is issued in writing at the time of registering and lodging an asylum application in cases where the applicant understands one of the 18 languages in which the written notice is available. Where no such written translation exists, the PBGB will provide the applicant with a relevant translation within 15 days. The interpreter will also provide the information verbally to the applicant.[213] In Germany, the information leaflet (which must be signed by the asylum applicant) is available in 41 languages. In the Netherlands, the processing notice is included in a leaflet providing information on the asylum procedure, which is available in several languages and is usually handed out during registering (registering and lodging are usually combined in the Netherlands). The leaflet can be further explained by a volunteer of the Dutch Council for Refugees or by an interpreter during the 'rest and preparation period'. France does not provide translations, but the association that accompanies applicants for international protection and helps them to complete their application explains how the French Office for the Protection of Refugees and Stateless Persons (OFPRA) collects the information and requests permission to share it.

Most of the Member States that provide the privacy notice in writing also provide the information to asylum applicants verbally.[214] In Ireland, applicants are issued with a privacy notice in writing, which applies throughout the protection procedure and is translated into 20 languages. The applicant is also verbally informed of the content of the Privacy Notice. The Slovak Republic on the other hand, only provides the privacy notice verbally in this phase. All Member States and Norway offer interpretation services when the privacy notice is provided verbally. Seven Member States[215] and Norway also provide digital information on data processing, with translation into several languages available in most cases.[216] For example, in the Netherlands, all of the information is provided in Dutch and in English, but on the website of the Dutch Council for Refugees it is available in Arabic, Dari, Dutch, English, Farsi, French, Somali and Tigrinya.

191 AT, CY, DE, EE, ES, FI, FR, HR, HU, LT, LU, LV, NL, PL, PT, SE, SI, SK and NO.
192 AT, CY, DE, EE, EL, ES, FI, HR, HU, LT, LU, LV, MT, NL, PL, PT, SE, SI, SK and NO.
193 CY, LU, LV, NL, PT, SK and NO.
194 EE, FI, LV, SK and NO.
195 AT, CY, LV.
196 AT, DE, EE, EL, FI, LU, LV, MT, NL, PL, PT, SE, SK and NO.
197 AT, DE, EE, EL, FI, HR, LU, LV, MT, NL, PL, PT, SE, SK and NO.
198 AT, CY, ES, FI, FR, HR, IT, NL, LU, LV.
199 LU, LV, PT, SK and NO.
200 AT, EE, FI, HR, LV, NL, SI.
201 AT, FR, NL.
202 EE, FI, HR, LV, SI.
203 FI, LV.
204 FI, HR.
205 EE, FI, LV, SI.
206 AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE, SI, SK and NO. In FI the privacy statements of the registers used by the police and border guard are available on the webpages of the police and border guard and can be consulted at any stage of the asylum procedure.
207 AT, BE, CZ, DE, EE, EL, FI, HU, IE, LT, NL, PT and NO.
208 CY, FI, LT, LV, NL, PL, SK.
209 HR.
210 EL, NL.
211 AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE and NO. In FI only the document 'Processing of personal data in reception services' is provided in writing.
212 AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PT and NO.
213 In EE, the registering and lodging of asylum applications happen concurrently.
214 CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT and NO.
215 AT, EE, EL, FI, IE, IT, NL.
216 AT, EE, EL, FI, IT, NL and NO.

Finally, 13 Member States and Norway reported providing specific training or guidance for the staff responsible for data management in respect of information collected in the lodging phase.[217] The Netherlands for instance, has a protocol for all personnel involved in the registration process, as well as online training for IND staff.

3.4. EXAMINING AN APPLICATION

Although most of the cross- checks against relevant databases are carried out during the lodging phase (see section 3.3), several Member States also cross-check personal information against national,[218] European,[219] and international[220] databases (Table 4) during the examining phase. At national level, information is most often cross-checked against police[221] and border guard databases,[222] and aliens' registers,[223] with some Member States checking criminal records again in this phase.[224]

Regarding European databases, 10 Member States and Norway engage in systematic cross-checking against the SIS[225] and nine against VIS[226] during this phase.[227] France, Hungary and Slovenia do not carry out systematic cross-checking against the VIS and SIS in any phase of the asylum procedure. None of the Member States cross-check data against Eurodac at this stage. In addition, four Member States reported consulting the Interpol SLTD database when examining an application.[228]

Similarly to the lodging phase, some of the issues encountered by Member States in cross-checking data during the examining phase include issues related to transliteration,[229] inconsistencies in the information,[230] and difficulties recording individuals with a single number or name across systems.[231] Slovenia highlighted the lack of information available in the national language, creating a problem for the decision maker, who has to assess and determine the relevance of information before asking for a translation.

Thirteen Member States provide applicants with a notice on the processing of the data collected from them during the examining phase (Table 5).[232] Luxembourg specifies that since the GDPR requires that individuals be informed once about the purposes for which their data are processed, they do not consider it necessary to inform applicants at each new stage. Estonia, Italy, Latvia, and the Netherlands note that applicants have their rights in relation to the processing of their personal data explained to them from the beginning of the asylum process. In the Netherlands, the information leaflet can be provided during the examining phase, if necessary. At the examining phase, public authorities in nine Member States[233] provide to asylum seekers the information on personal data collected.

As in previous phases, information on personal data collected is provided in digital, verbal and written formats, depending on the Member State. The information is provided verbally in 13 Member States,[234] which also offer interpretation services. Interpretation is provided by public authorities in 10 Member States.[235] Sweden uses independent interpretation providers (under an arrangement with Swedish governmental agencies). Eleven Member States provide information in writing,[236] and written translations are available in virtually all of these. Finally, the information is provided digitally in five Member States,[237] all of which also offer translations. In Belgium, for example, translation is provided by the Office of the Commissioner General for Refugees and Stateless Persons (CGRS), and in the Netherlands it is provided by the public authorities involved in the asylum process, whose websites are all available in Dutch and English (with the website of the Dutch Council for Refugees providing more languages).

Eleven Member States provide specific training or guidance for the staff responsible for data management with respect to information collected in the examining phase.[238] Estonia specified that such training targets the staff responsible for data processing in all phases.

Table 5 provides an overview of the phases of the asylum procedure at which a privacy notice is provided, as well as the format of the privacy notice (written, verbal, digital) and the availability of translation/interpretation services.

217 AT, DE, EE, EL, FI, FR, IE, IT, LV, NL, PL, PT, SK and NO.
218 AT, CY, EE, ES, FI, HR, HU, LT, LV, PT, SE, SK.
219 EE, EL, ES, FI, HR, HU, LV, PT, SK and NO.
220 EE, LT, LV, PT.
221 FI, HU, LT, SE.
222 EE, FI, HR, HU, LT, SK.
223 EE, HR, LT, PT, SK.
224 EE, FR, LT.
225 EE, EL, ES, FI, HR, LT, LV, PT, SE, SK and NO.
226 EE, EL, ES, FI, LT, LV, PT, SE, SK and NO.
227 EE, EL, FI, HR, LT, LV, PT, SE, SK and NO. As HR does not have access to VIS, cross-checks are only carried out against SIS.
228 EE, LT, LV, PT.
229 HR, LT, SE.
230 HR, SI.
231 FI, SE.
232 CY, EL, DE, FI, FR, HR, IT, LT, LV, NL, PT, SE, SK.
233 BE (CGRS), DE, EE (PBGB), FI (Immigration Services), FR (OFPRA), HR (Ministry of the Interior), LT, LV (Asylum Affairs Division), SE, SK (Migration Office).
234 CY, DE, EE, EL, FI, FR, HR, IT, LT, LV, NL, PT, SE.
235 BE, EE, EL, FR, HR, LT, LV, NL, PT, SE.
236 CY, DE, EE, EL, HR, IT, LV, NL, PT, SE, SK.
237 BE, EL, FI, IT, NL.
238 DE, EE, EL, ES, FI, LV, NL, PL, PT, SE, SK.

Table 5. Provision of processing/privacy note about personal data collected in three phases

	Registering phase	Lodging phase	Examining phase
Provision of processing/privacy note	CZ, DE, EE, EL, ES, FR HR, HU, IT, NL,[239] PT, SE	AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE, SI, SK and NO	CY, DE, EL, FI, FR, HR, IT, LT, LV, NL, PT, SE, SK
Verbally	CZ, DE, EE, EL, FR HU, IE, IT, NL, PT	CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SK and NO	CY, DE, EE, EL, FI, FR, HR, IT, LT, LV, NL, PT, SE
Interpretation available when provided verbally	CZ, EE, EL, FR HU, IT, NL, PT	CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SK and NO	CY, DE, EE, EL, FI, FR, HR, IT, LT, LV, NL, PT, SE
Digitally	EE, EL, IT, NL and NO	AT, EE, EL, FI, IE, IT, NL and NO	BE, EL, FI, IT, NL
Translation available when provided digitally	EE, EL, IT, NL	AT, EE, EL, FI, IT, NL and NO	BE, EL, FI, IT, NL
Writing	CZ, DE, EE, EL, ES, FR HR, HU, IT, NL, PT, SE	AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PL, PT, SE and NO	CY, DE, EE, EL, FR HR, IT, LV, NL, PT, SE, SK
Translation available when provided in writing	CZ, DE, EE, EL, HR, HU, IT, NL, PT	AT, BE, CY, CZ, DE, EE, EL, FI, HR, HU, IE, IT, LT, LV, NL, PT and NO	CY, DE, EE, EL, IT, LV, NL, PT, SE, SK

239 In NL, the registering and lodging phases are combined (see section 3.3).

4. DATA QUALITY ASSESSMENT AND SAFEGUARDS

This section looks at data quality management and safeguards in the asylum procedure. Section 4.1 provides information on whether, how (tools and methods) and by whom data quality is assessed in the different phases of the asylum procedure. Section 4.2 reviews existing supervision and compliance mechanisms for the protection of data collected and summarises how applicants exercise their right to access, rectify and erase their data stored in national information systems.

4.1. DATA QUALITY MANAGEMENT

The quality of alphanumeric and biometric data collected during the asylum procedure is assessed for accuracy, timeliness, completeness, consistency, duplication and validity (among others) in the vast majority of the Member States and Norway.[240] This assessment takes place throughout the asylum procedure,[241] or during one or more of the specific phases: registering,[242] lodging,[243] and examining.[244] In Finland and the Slovak Republic, for example, this assessment takes place once and twice per year, respectively, as part of overall quality control. In the Netherlands, a selection of asylum procedures is assessed for data quality every week. Five Member States make no provision for data quality assessment.[245]

National competent authorities have a wide range of quality control tools and methods to assess the quality of data collected and stored during the asylum procedure. In Sweden, quality assessments are carried out on a regular basis and focus on specific areas (e.g. registration or interview), with the method depending on the dataset assessed. Several Member States use a data comparison approach, where data collected are checked against data declared, previously collected data (including data stored in databases), or travel documents.[246] In some cases, applicants are themselves involved in the quality assessment process. In Belgium, applicants are asked to confirm the accuracy of data collected, for example, and in Ireland, at the end of the lodging phase, the applicant has to confirm in writing that their details are correctly recorded (they then receive a copy of the details). Five Member States reported having automated data quality checks in place.[247] In Slovenia, systematic checks are carried out at the registering phase by the police, using special software that generates alerts where inconsistent data are identified. In Spain, a team of administrators check data collected by police officers during the registering phase to ensure its coherence, completeness and accuracy before entering that data in the Asylum Register.

Box 7 Establishing identity and ensuring better data quality in Germany

In order to improve the identification process, the BAMF introduced assistance systems within the framework of the programme 'Integrated Identity Management - Plausibility, Data Quality and Security Aspects (IDM-S)'. These systems provide supporting information within the framework of clarification of the facts. Case officers thus have access to additional indications that help them to determine the facts of the case. The IDM-S tools include:

- Image biometrics;
- Name transliteration and analysis or web-based transcription service;
- Speech biometrics;
- Evaluation of mobile data carrier.

These assistance systems are based on modern data analysis methods. The information collected from asylum seekers in the asylum procedure can be immediately checked for plausibility, leading to better data quality. If doubts remain about the identity of applicants, BAMF consults language experts to carry out a check by means of language and text analysis. Such cases can be reported to the competent specialist unit within the security group at BAMF, if necessary. The 'Operational Cooperation with Federal and State Security Authorities' unit works closely with various national authorities from the field of internal security within the framework of the Joint Counter-Extremism and Counter-Terrorism Centre (GETZ) and the Joint Counter-Terrorism Centre (GTAZ). In addition, since the entry into force of the Second Data Exchange Improvement Act, the asylum consultation procedure (AsylKon) is used in place of automated data-matching with the security authorities.

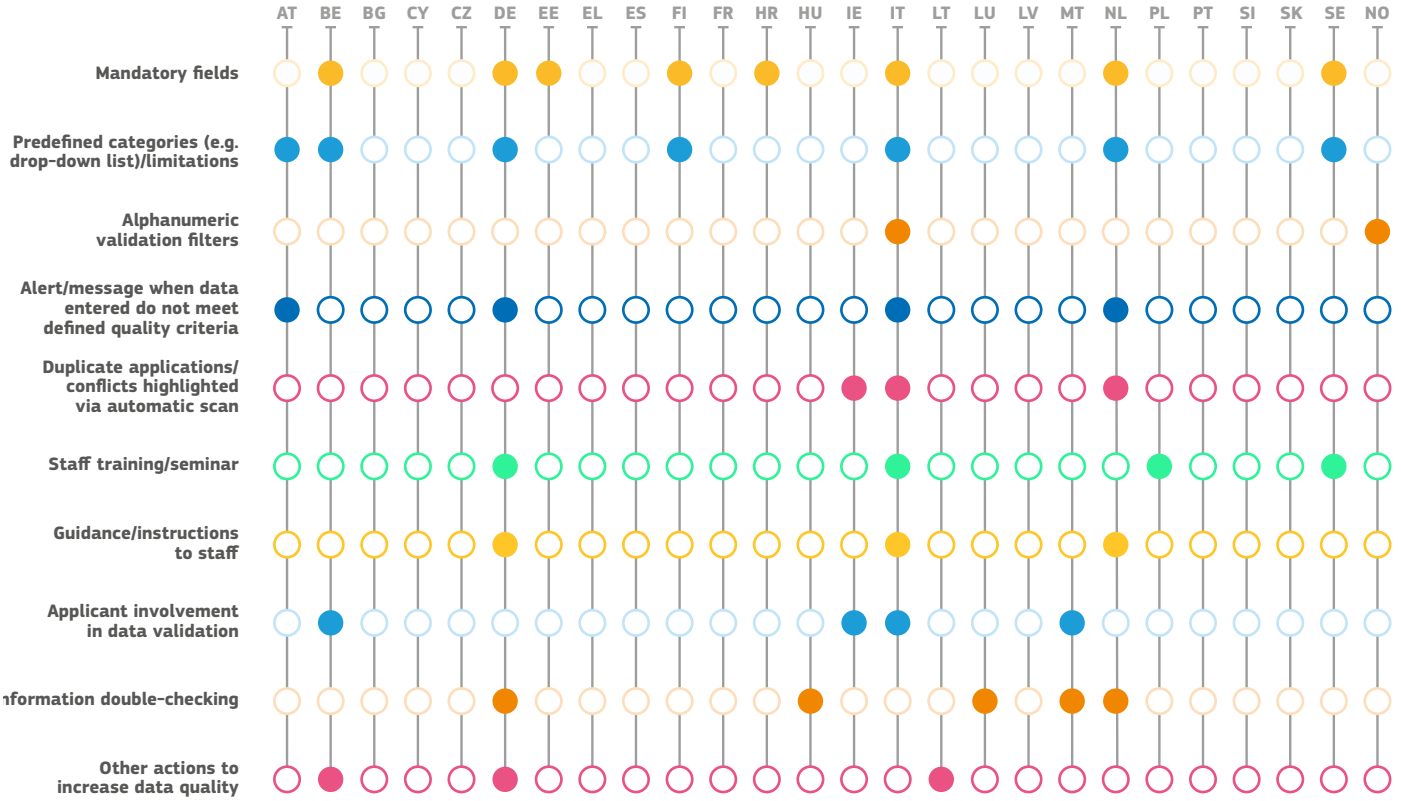
240 AT, BE, CZ, DE, EE, EL, ES, FI, FR, HR, IE, IT, LU, LV, MT, NL, SE, SK, SI and NO.
241 AT, BE, DE, HR, IE, LV, NL, SE and NO.
242 ES (errors detected during the process are corrected), HR, IT, SI.
243 FR, HR, LU, MT.
244 FR, HR, LU.
245 CY, HU, LT, PL, PT.
246 AT, BE, CZ, DE, HR, IT, MT, NL, SI.
247 DE, IE, LV, NL, SI.

Most Member States and Norway have centralised data quality assessment processes.[248] In the Slovak Republic, the assessment is partly centralised (during the asylum procedure quality assessment) and partly decentralised (ad hoc controls to assess data quality in information systems). The remaining Member States following a decentralised approach[249] reported having information flow mechanisms in place to ensure that the actors involved are informed of data amendments and changes. In some cases, information is shared with relevant actors automatically[250] and/or manually.[251] In other cases, the relevant actors have direct access to the information stored and are notified when information is modified.[252]

In the majority of the Member States and Norway, measures to ensure data quality are not only retroactive but implemented from the very beginning of the procedure.[253] In just four Member States, quality assessment measures are solely retroactive.[254]

Most Member States and Norway have preventive measures in place to ensure that the correct information is collected and stored at the beginning of the asylum procedure.[255] Such measures range from mandatory fields to predefined fields with drop-down lists, and guidance and training for the staff involved (Figure 3).

Figure 3. Preventive measures to ensure the collection of correct data[256]



4.2. DATA PROTECTION SAFEGUARDS: SUPERVISION AND INDIVIDUAL RIGHTS

EU data protection law[257] requires the Member States and Norway to have a mechanism for data protection supervision, including data collected and processed as part of the asylum procedure. Of those countries that provided more information on this mechanism, some Member States and Norway, report that the mechanism is part of the general national data protection supervision procedures entrusted to the DPA,[258] while others report a specific data

248 AT, CZ, DE, EE, EL, ES, FR, IE, IT, LU, LV, MT, SE, SI, SK (partially) and NO.
249 BE, FI, HR, NL, SK (partially).
250 DE, NL.
251 ES, FI, NL, SK.
252 DE, HR, NL.
253 AT, DE, EL, FI, HR, IE, IT, LU, LV, MT, SI, SK and NO.
254 FR, HU, NL, SE.
255 AT, BE, DE, ES, HR, FI, HU, IE, IT, LU, LV, MT, NL, SE, SI and NO.
256 NL uses a unique V-number for all communication by organisations cooperating in the asylum process. That number is known by the asylum seeker and avoids confusion of data/ duplicate registrations.
257 In particular, GDPR, Articles 51-59 and its predecessor Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, p. 31, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&-from=EN, last accessed on 28 May 2021.
258 BE, HR, CY, CZ, HU, IE, IT, LT, PT, SI, SK and NO.

protection supervision and compliance mechanism for data collection in the asylum procedure.[259] In five Member States, supervision and compliance take place at both the level of the migration authority and within the framework of the supervision conducted by the national DPA.[260] In those Member States reporting a specific data protection supervision mechanism for data collection in the asylum procedure, the authority in charge of migration matters has a data protection officer responsible for data protection compliance.[261]

In a number of Member States and Norway, supervision takes place through inspections[262] and audits[263] (see Box 8). In Cyprus, both the Protection Commissioner and the national audit office can initiate such an audit.

Box 8 Data protection monitoring and compliance mechanism in Norway

The DPA in Norway is responsible for data protection supervision and can take action on its own initiative. It may undertake an audit on the basis of a complaint from a data subject, a reported deviation that feeds into the asylum process, or following a request from the Norwegian Directorate of Immigration related to a privacy impact assessment of a system or process in the asylum procedure. Several safeguards are in place within the Immigration Service of the National Police to ensure data security in the processing of personal data during the asylum procedure. Personnel with access to those data are required to complete an online training course and to commit to policies on the processing of personal data and the different systems in which personal data are processed. Any suspicion or detection of a personal data breach is reported by personnel using the deviation system and is then assessed and addressed to limit and mitigate the breach. Use of personal data and access to the asylum procedure systems are monitored by the head of information security. Suspicious or deliberate misuse of employee access will result in access being revoked. Depending on the context of the data breach, the employee will be required to retake the necessary training to have their access rights granted again.

In 11 Member States, the DPA (or a similar entity) has already monitored the lawfulness of the processing of data stored in certain databases used in the asylum procedure, with assessment ongoing in Luxembourg and Slovenia at the time of drafting this study.[264] In most cases, the results and recommendations of such assessments led to changes in data management, at least to some extent. In Austria and Finland, no serious deficiencies were detected but the recommendations of the DPA were implemented, while Sweden improved the processing of personal data as a result of the monitoring exercise. Slovenia's inspection procedure for the processing of applicants' accommodation data is currently underway. Initial comments on the lack of a legal basis for collecting these data has led to the preparation of an amendment to the Slovenian International Protection Act. Reports on the inspections/assessments are not publicly available.

In addition, to ensure respect for applicants' rights under data protection law, the Member States and Norway have implemented certain data protection safeguards to ensure respect for applicants' rights. Some examples of these safeguards include: encrypting data,[265] only sharing data with external parties under very limited circumstances,[266] only sharing requested data rather than the whole file with relevant governmental organisations,[267] and giving access only to authorised users.[268] In Finland, for example, a user must have legal grounds to consult or process information related to a case (see Box 9). Some other safeguards adopted by the Member States and Norway include guidelines and training for the staff of migration/asylum authorities (such as a GDPR programme for IND staff in the Netherlands),[269] and personnel liability for data protection breaches in Finland and Latvia.

Box 9 Supervision mechanism in Finland

The Finnish Immigration Service contains a Data Protection Section and a Data Protection Officer. The Data Protection Section assists management in the preparation of data protection matters, advises and supports the units, provides guidelines and training to personnel, ensures that the rights of data subjects are respected in the Finnish Immigration Service's activities, and supervises compliance with data protection legislation.
Data protection is supervised through technical measures (e.g. restricting access rights of users, information not given over the phone) and organisational measures (e.g. staff liability for acts, staff training).
Use of the Asylum Seeker Reception Client Register is supervised, and information is shared with the Finnish Immigration Service over an encrypted connection only. User access rights are individual and are granted by the Finnish Immigration Service. The Reception Unit has the legal power and resources to supervise, conduct log inspections, develop guidelines, organise training and develop user manuals to improve data processing.
Use of the National Police Information System is restricted. Reports on applications for international protection are stamped as confidential and information is available only to the parties concerned.

The GDPR grants applicants for international protection the right to request access to, rectification and erasure of their personal data stored in national systems. In most cases, the GDPR is supplemented by national law to enable individuals whose personal data are collected, stored and processed (data subjects) to exercise these rights.[270] In some Member States, applicants can receive a copy, print-out or

259 AT, EE, FI, PL.
260 DE, ES, LU, NL, SE.
261 DE, EE, FI, NL, LU, PL, SE.
262 CZ, DE, FI, HR, IE, SK and NO.
263 AT, CY, CZ, DE, FI, IE, SE, SI and NO.
264 AT, CY, CZ, DE, EE, FI, HU, IE, IT, NL, SE. In BE the assessment of the VIS was postponed until 2021 due to the COVID-19 pandemic.
265 CZ, DE, EE, IT, SK.
266 AT, CZ, FI, HR, NL, SK.
267 HR, DE, NL.
268 AT, CZ, DE, EE, FI, HR, IT, LV, NL, SI, SK and NO.
269 DE, FI, IE, NL and NO.
270 BE, CZ, DE, EE, HR, FI, FR, IE, IT, LT, LV, NL, PL, SE, SI, SK and NO.

information in writing,[271] the information may also be read to the applicant, as is the case in Finland for data in the police register. Erasure of data is not possible in all cases. The GDPR[272] allows for some exceptions to the right to erase personal data, including complying with legal obligations, for archiving purposes, and for the establishment, exercise and defence of legal claims. Some Member States have made used of those exceptions and do not allow the erasure of certain categories of asylum applicants' data.[273] In Finland, for example, no data are erased from police registers or the Register of Aliens. Inaccurate personal data can be retained along with the corrected data, as long as it is necessary to safeguard the rights of the registered person, another concerned party or the data controller. In Italy and Malta, erasure is prevented so as to minimise abuse of the system whereby the same person re-applies for international protection multiple times. In the Netherlands, applicants for international protection can request the erasure of data, although some categories of data are protected by the Archive Law for demographic and historical purposes and cannot be legally destroyed (e.g. asylum/immigration decisions, court decisions, marriage certificates). Similarly, in Croatia, the erasure of data is not possible for all categories of data (e.g. data necessary for the purpose of archiving, data needed to continue with administrative procedures).

An applicant wishing to access, rectify or erase their data should provide proof of identity and, in case of a rectification request, the appropriate supporting documents.[274] Applicants can submit their requests to the competent authority in person,[275] electronically via email,[276] through an online form,[277] or by post.[278] In Finland, if the applicant does not have a document that reliably proves their identity, they must visit the Finnish Immigration Service's customer service point, where identity is ascertained on the basis of the information and photograph in UMA.

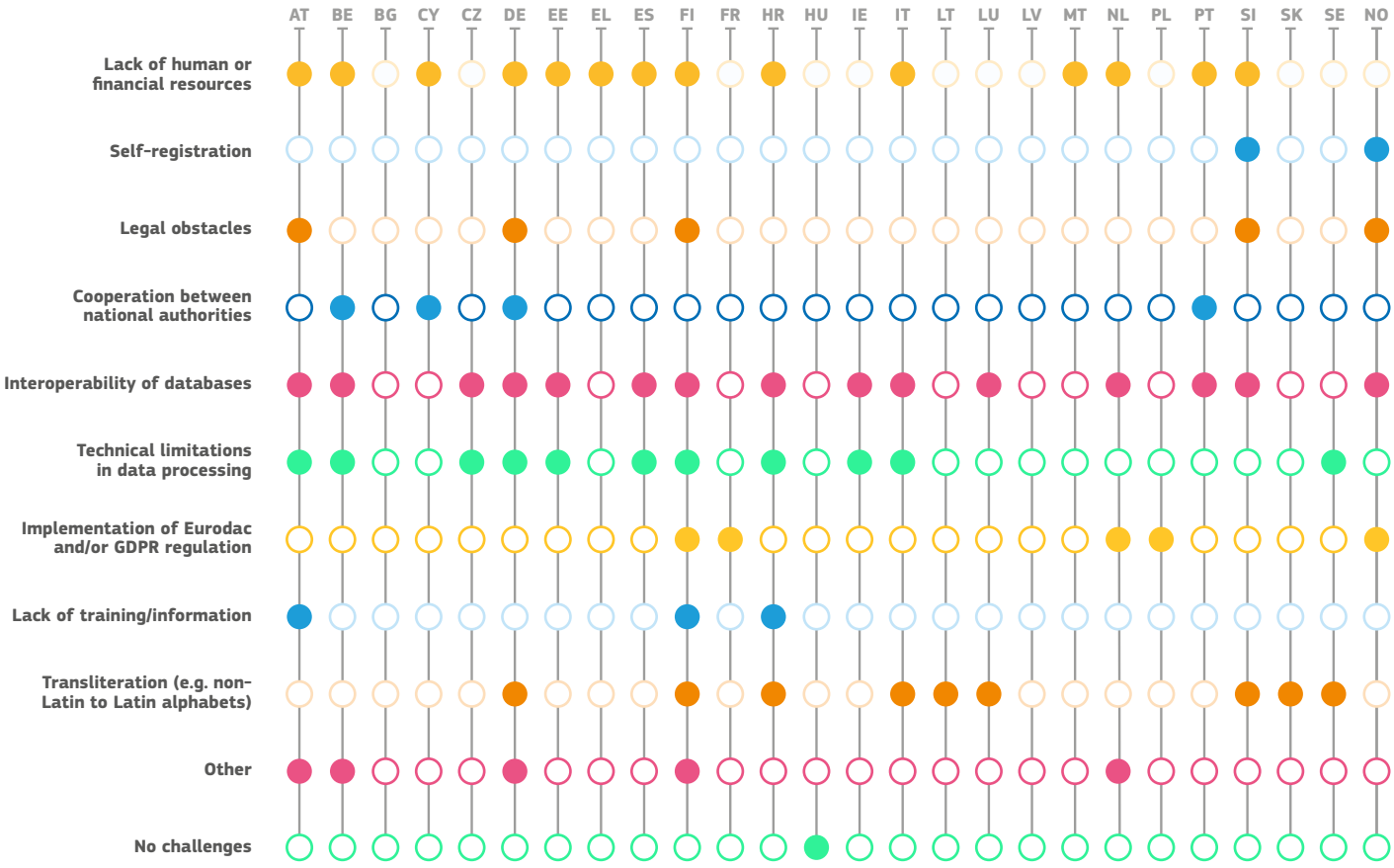
Despite the possibility to exercise their right to request access, rectification and erasure of their personal data, some Member States reported that no such requests have been made by applicants to date.[279] Other Member States did not have available statistics on these requests.[280] Only Norway reported that the responsible authority had received 40 such requests since the implementation of the GDPR.

271 BE, CZ, FI, HR, IE, LT, LU, NL.
272 GDPR, Article 17(3).
273 FI, HR, IT, LV, LU, MT, NL.
274 BE, CZ, DE, FI, HR, IE, LT, LU (only rectification possible), MT.
275 FI, HR, LT, LV, LU, NL, PL, SE, SK.
276 CZ, DE, EE, FI, HU, IE, LT, LU, PL, SE, SK.
277 BE, EE, ES, NL, SE.
278 CZ, DE, FI, IE, EE, LT, LU, NL, PL, SK.
279 BE, EE, LU, MT, PT, SK.
280 AT, DE, ES, FI, FR, HR, IE, LT, NL, SE, SI, SK and NO.

5. CHALLENGES IN DATA MANAGEMENT

Section 5 summarises the various challenges that Member States and Norway have encountered in relation to data management since 2014, together with some of their responses. It highlights a number of challenges that remain unaddressed, as well as some Member States' initiatives to address them.

Figure 4. Overview of challenges



The most common challenges experienced by the Member States and Norway with regard to data management in the asylum procedure relate to the lack of human or financial resources[281] and the interoperability of databases.[282] A lack of human resources can impact the competent authorities' capacity to process applications.[283] This issue relates to different actors involved in the asylum process, with varying consequences. In Finland, staff shortages in the Data Protection Section may affect the amount of data protection training and guidance. Italy reported that limited space means that the level of privacy necessary for data collection and management is suboptimal, while the lack of human and financial resources may delay the compilation of statistical data and impact data quality assessments.[284] Reliance on external consultancy firms may also create challenges, with Belgium reporting the delayed development of the 'Evibel New Generation' database at the Immigration Office due to turnover of external staff and changes in methodology and direction.

281 AT, BE, CY, DE, EE, EL, ES, FI, HR, IT, MT, NL, PT, SI.
282 AT, BE, CY, CZ, DE, EE, FI, FR, IE, LU, NL, PT, SI and NO.
283 BE, DE, IT, NL, SI.
284 HR, MT.

On the interoperability of databases, Member States reported difficulties in cross-checking applicants' data across databases managed by different authorities.[285] The issue was reported in different phases of the asylum procedure and related to the use of different categories of data collected and shared (e.g. different formats) (see section 3). For instance, Finland reported that when registering an application, police must take applicants' fingerprints four times in order to be able to cross-check them against different registers. Ireland reported that interoperability challenges have arisen due to the current architecture of case processing management systems. As a result, the interrogation of the various systems is not as streamlined as it could be. The Directorate of Immigration in Luxembourg operates three different databases,[286] complicating cross-checking at times.

The emerging interoperability of EU information systems may create issues for automated data processing and result in discrepancies in data entry rules at EU and national level. The Netherlands reported difficulties related to preparation for European regulations leading to the implementation of the European Travel Information and Authorisation System (ETIAS)[287] and other systems using biometric and biographical data to establish connections. These data can lead to many potential hits. Italy noted issues in the use of Eurodac, particularly the inadequate speed of data processing and poor data transmitted (information about the final outcome of asylum applications lodged by applicants in other Member States is missing). Sharing files between different offices in different formats also highlights inconveniences. In Belgium and Germany, for example, the mixed use of paper and electronic files has proven costly and time-consuming when exchanging information on asylum applicants. Similarly, in Lithuania, the Directorate of Immigration still works only with paper files, although this does not hinder information exchange, as all the necessary data from the paper files are fed into databases. Lithuania is currently developing a Migration Information System that, once operational, will contain all data on asylum applicants and eliminate paper files. In Ireland and Italy, a related challenge is the limited collection of data in a format that is searchable and can thus be used to filter claims and apply triaging or channelling methodologies. In Luxembourg, the Directorate of Immigration, despite using databases for some data, still works on paper files. As a consequence, not all necessary data are fed into one of the databases and paper files must sometimes be consulted for specific information not available elsewhere.

Technical limitations in data processing present a challenge to data management in several Member States.[288] Six Member States noted issues related to old equipment and a lack of technical capacity, which affected or still affects their capability to handle cases quickly and efficiently, and to deliver exact statistical data on asylum applications.[289] Technical limitations may mean that digital material provided by applicants in support of their application (e.g. USB flash drive or video clips) may not be stored in national databases, as reported by Finland.

Eight Member States reported facing challenges in relation to transliteration from Cyrillic or Arabic to Latin alphabets, and vice versa.[290] Specific challenges include poor data quality due to a lack of interpreters and tools for transliteration,[291] especially when applicants enter the country without documents, or with passports issued in their mother tongue only. The lack of efficient transliteration methods can lead to multiple registrations for a single applicant (Germany and Sweden) and, in some cases, can make it difficult to cross-check applicants' information across EU databases, as Member States translate names in different ways and applicants' records are not aligned. In Lithuania, the issue of transliteration is solved by cross-checking data not only according to a foreigner's name and surname, but also according to their date of birth and image (if any). The Slovak Republic mentioned a challenge related to the conversion of dates from the Solar Hijri calendar to the Gregorian calendar.

Several Member States and Norway reported challenges related to the implementation of the GDPR.[292] More specifically, they described ongoing issues related to the (slow) alignment of national legislation with the GDPR.[293] In Finland, enforcement of the Act on the Processing of Personal Data in Immigration Administration was delayed, as were measures to inform data subjects in line with the GDPR. The Netherlands reported that problems can stem from different interpretations of GDPR provisions across different organisations sharing information on applicants, and these may delay processes (see section 3).

Legal obstacles were mentioned by a few Member States and Norway as challenges to data management in the asylum procedure.[294] Germany reported issues due to the lack of a legal basis for the collection of certain data categories or the exchange of data between authorities. Several Member States reported problems with cooperation between national authorities,[295] as well as a lack of training and information on data management issues.[296]

285 BE, DE, IE, SI and NO.
286 One for immigration and return purposes, including for family reunification; one for the management of the asylum procedure; and a third for the sole purpose of asylum statistics.
287 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, OJ L 236, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1240, last accessed on 28 May 2021.
288 AT, BE, CZ, DE, EE, ES, FI, HR, IE, IT, SE, SI.
289 BE, DE, EE, IT, HR, SE.
290 FI, HR, IT, LT, LU, SE, SI, SK.
291 LT, SE, SI.
292 FI, FR, NL, PL and NO.
293 FI, FR, NL.
294 AT, DE, FI, SI and NO.
295 BE, CY, PT.
296 FI, HR, NL.

Some of these challenges remain outstanding in a number of Member States and Norway.[297] Ongoing issues include the interoperability of national databases, insufficient use of information systems for data storing, and the digitalisation of systems. In order to alleviate challenges in the interoperability of national and/or international databases, Belgium is exploring possibilities for future electronic data transfers between the competent authorities. Finland is developing a project to cross-check fingerprints between different registers, as well as enhancing the use of national and international biometric registers in asylum examination procedures. Slovenia is working on quicker and easier data traceability through an interoperable solution between the police and asylum databases. In Luxembourg, work is in progress to integrate the asylum database into the immigration database in order to increase interoperability while enhancing security. In Ireland, the Department of Justice is exploring the potential reform of its information technology strategy, which includes the International Protection Office. With respect to the insufficient use of information systems for storing data, Czech Republic is gradually moving towards digitalisation, and while Spain's Asylum Register does not hold all data needed to fulfil its statistical duties, it will migrate to a new and more powerful database this year. Italy is developing and implementing a new system, merging different databases into one.

297 BE, CY, CZ, DE, FI, HR, IE, LU, LV, MT, NL, PT, SE, SI and NO.

6. RECENT DEVELOPMENTS RELATING TO DATA MANAGEMENT

Section 6 presents the changes and recent reforms to the asylum procedure. Section 6.1 provides an overview of the main changes adopted by Member States and Norway in response to challenges in data management and information on whether or not those changes achieved their intended results. The remaining two sections explore the contingency measures introduced by Member States to deal with the high influx of applicants for international protection (section 6.2) and the policies adopted to reduce the negative impacts of COVID-19 on data management in the asylum procedure (section 6.3).

6.1. CHANGES AND REFORMS IN DATA MANAGEMENT

Since 2014, most Member States have introduced changes to their data management in the asylum procedure.[298] These changes primarily relate to the digitalisation of data management,[299] implementation of the GDPR,[300] and database organisation (e.g. introduction of new databases or changes to existing databases).[301]

Six Member States sought to increase the digitalisation of data management to improve the traceability of the data collected in the asylum procedure and to accelerate and streamline the registration of applications.[302] Croatia's Ministry of the Interior introduced a centralised system for the storage and digitalisation of all documentation related to the international protection procedure. The system improved the quality and speed of the procedure by making the digitalised paperwork accessible, depending on the phase of the procedure, to the competent organisational unit. This is considered good practice and has been integrated as a standard procedure. Greece noted the introduction of electronic self-registration for applicants, which has improved the efficient management of applications.

A series of reforms were adopted to align national rules for the processing of personal data with the GDPR.[303] In Estonia, for example, a data protection officer was appointed at the PBGB. These changes were incorporated as standard procedures in all of the Member States mentioned.

Several Member States introduced new databases for data management in the asylum procedure. In most cases, the new systems unified pre-existing databases, thus mitigating the issue of the interoperability of databases and ensuring smooth communication among all asylum actors.[304] These examples of good practices were integrated as standard procedures as they improved the interoperability between different systems, data quality, speed of information transmission and access to necessary data, speeding-up asylum decisions.[305] In Germany, two major legal changes resulted in fundamental changes to the interoperability of databases, including uniform technical infrastructure, one Core Data System and additional access rights for more actors, frontloading of data collection and data quality standards. Austria referred to the introduction of the Integrated Administration of Aliens' System as an example of good practice, as it reduces the administrative effort required for asylum procedures and has become a standard tool in the country.

Three Member States reported that some of these changes/reforms were the result of the introduction of channelling of applications.[306] Finland developed keywords and automatic functions to channel applications to the right 'baskets' (see Box 1), while Latvia is working on load accounts connected to its Register of Asylum Seekers in order to facilitate the distribution of cases among caseworkers and improve compliance with procedural time limits.

298 AT, BE, CZ, DE, EE, EL, ES, FI, FR, HR, IT, LV, MT, NL, PL, SE.
299 DE, EL, FI, HR, LV, NL.
300 BE, CY, CZ, EE, FI, PL, SE.
301 AT, BE, CZ, DE, ES, FI, FR, HR, IE, IT, LU, MT, NL, SI.
302 DE, EL, FI, HR, LV, NL.
303 BE, CY, EE, FI, PL, SE.
304 AT, DE, FR, HR, IT, MT, NL, SI.
305 DE, FR, HR.
306 FI, FR, LV.

Box 10 Changes in data management in the international protection procedure introduced in the Netherlands since 2014

The Netherlands has adopted a series of reforms to respond to challenges in its identification and registration (I&R) processes. Other amendments relate to the types of data collected in the immigration process.

2014: Legislative amendments were adopted in relation to the extended use of biometric data in the immigration process to establish the identity of third-country nationals. It is now possible to take and process facial images and fingerprints of all third-country nationals and store them centrally in a register that is accessible to cooperating organisations. This reform has become part of the standard operating procedure.

2015: The Basic Facility for Identity Establishment (*Basisvoorziening Identificatie* - BVID) Kiosk was introduced to integrate the I&R processes for immigration law and criminal law into one system. Depending on the situation and nationality of persons identified at the BVID Kiosk, the criminal law register and/or immigration law register are consulted and amended.

The BVID Kiosk was integrated as a standard procedure and its implementation is regarded as a good practice by experts of the Ministry of Justice and Security because it verifies identity more reliably.

2017: Earlier registration in the BRP for applicants for international protection who are expected to stay in the country for at least four months and whose identity has been established. Applicants then receive a citizen service number sooner so that they can arrange government services. Previously, applicants awaiting a residence permit and residing in a reception centre were registered in the BRP after six months of stay. The earlier registration has been integrated as a standard procedure.

2019 - 2020: New changes were introduced to renew the I&R process. A 'vestibule' was established, where applicants and their luggage are subjected to a search: attention is paid to objects such as identity documents and data carriers, which may assist in establishing the person's identity. The different cooperating organisations are brought together on a multidisciplinary platform, where they process information and decide on the next steps of the application.

The renewed I&R process, including the vestibule and multidisciplinary platform, is considered a good practice by the Dutch Council for Refugees, as it allows swift exchange of more and better information during the registering phase and helps cooperating partners to conclude the procedure.

6.2. CONTINGENCY MEASURES

Since 2014, a number of Member States and Norway adopted contingency measures for data management, seeking to accelerate and ease the process in times of high influx of applicants, while also making their asylum systems crisis-proof.[307] Most of these 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.[308] For instance, some Member States use accelerated procedures to quickly collect the most necessary personal data and make the appropriate cross-checks to ensure that no applicant is unregistered,[309] while others introduced self-registration procedures.[310] Greece allows for the participation of EASO staff where there is an urgent need for administrative procedures to examine applications. In Finland, the government may decide that persons whose requirements for entry or identity are unclear may be sent to a different registration centre and the police or border control authority may extend the registration time limit to 10 working days.

Box 11 'Flexible asylum system' in the Netherlands

Following their experiences of managing a high influx of applications in 2015 and 2016, the parties that play a role in the migration process (organisations falling under the Ministry of Justice and Security, municipalities and civil society organisations) are developing a so-called 'flexible asylum system' through a programme called *Flexibilisering Asielketen*.[311] This aims to create a system that responds more flexibly to major changes in the influx of asylum seekers.

307 AT, CZ, DE, EL, FI, FR, IT, LV, NL, SE, SI and NO.
308 AT, CZ, EL, FI, SE and NO.
309 AT, IT, SE.
310 EL and NO.
311 Rijksoverheid, 'Programma Flexibilisering Asielketen', https://www.rijksoverheid.nl/onderwerpen/migratie/programma-flexibilisering-asielketen, last accessed on 10 June 2021. (Website only available in Dutch).

Five Member States reported having operational contingency plans and protocols in place to ensure proper coordination and efficient use of resources in case of high pressure on the asylum system.[312] In Finland, the Reception Unit of the Finnish Immigration Service is responsible for the national contingency plan for the reception of asylum seekers and for the establishment of registration centres. The police and the Finnish Border Guard also have contingency plans. The Asylum Unit of the Finnish Immigration Service is preparing an operating model for processing asylum applications in the event of a mass influx of migrants. In the Netherlands, the Operational Coordination Centre for Foreign Nationals (KOCV) (a logistics centre representing all partners involved in the asylum system) was established at the time of the increased influx in 2015. It has been maintained, together with the 'High influx of asylum seekers' contingency plan' adopted in 2016. Latvia developed an action plan to reinforce interinstitutional cooperation in the event of a significant increase in the number of asylum seekers.

6.3. IMPACT OF COVID-19 ON DATA MANAGEMENT IN THE ASYLUM PROCEDURE

The COVID-19 pandemic saw several Member States and Norway introduce changes in their data collection and management during the asylum procedure.[313] The most important reforms related to:

- Temporary suspension of the registration of asylum applications.[314] In Italy, only those applications selected for the relocation procedure were lodged, and the lodging took place through remote interviews conducted by EASO caseworkers. In Finland, registrations were delayed only if an applicant had symptoms of respiratory infection, and there was a temporary suspension of asylum interviews until protection solutions were adopted in all facilities. Croatia created an auxiliary register for self-isolation of applicants that was incorporated into existing databases and updated on a regular basis.
- Digitalisation of some steps of the asylum procedure, such as remote interviews with applicants.[315] One example is the use of Skype, with both the applicant and the agency staff present in the same office, but in different rooms. This change took into account national prioritisation, security issues and applicants' individual needs and vulnerabilities in order to avoid conducting particularly sensitive interviews through a screen.[316] Greece established a digital platform where applicants can carry out a series of administrative actions (i.e. making appointments, renewing international protection cards and self-registration). Austria had anticipated the modernisation of asylum procedures prior to the COVID-19 pandemic (e.g. procurement of video conference equipment to allow remote audiovisual interviews of applicants). These plans were implemented sooner and to a wider extent than originally planned.
- Sweden began to collect 'flat' rather than 'rolled' fingerprints in order to minimise physical contact between staff and applicants.

312 CZ, FI, LV, NL, SI.
313 BE, DE, EL, FI, HR, LT, NL, SE and NO.
314 BE, EL, FI, IT.
315 AT, BE (decision taken by the CGRS, but suspended by the Council of State as this practice requires legal amendments), EE, EL, FI, HR, IE, IT, NL, SE and NO.
316 SE and NO.

7. CONCLUSIONS

A smooth and fast registration and identification procedure that maintains data accuracy is essential for the adequate functioning of the asylum procedure. This study examined data management approaches in the asylum procedure, including data protection safeguards, challenges faced by Member States, and procedural changes introduced to enhance data-sharing among asylum authorities (and others).

Although there are some differences in the types of data collected by Member States as part of the asylum procedure, some common categories of data are collected by most Member States. For example, all Member States collect data on current and/or birth names, birth date, citizenship, contact details, health status and some categories of biometric data (photo and fingerprints) and most Member States collect information on family members already in a Member State, vulnerabilities, and level of education. Very few collect data on a person's religious name, social media profiles, applicants' financial resources and criminal records, however.

The phases at which data are collected vary between Member States, although a trend in frontloading data collection was observed for some categories, including name, biometrics, place of birth and supporting documents (e.g. passport, travel documents). Several Member States considered frontloading to be good practice, as it allows the authorities to obtain the necessary information in the early phase of the asylum procedure and to prioritise certain categories of applications, while saving on administrative capacity and allowing other competent institutions immediate access to the data. Where asylum applications are made to authorities that are not competent to register an application, data are not usually collected, with applicants instead referred to the competent authority for registering, where the data collection process begins. If data are collected at the time the application is made, the information is typically passed to the competent authorities in the subsequent phases. Due to the trend in frontloading, an increased amount of data is collected by border guards and local police, as the main authorities responsible for registering and lodging applications. On the other hand, during the examining phase, data are primarily collected by immigration offices and the competent ministries in most Member States.

Although data on asylum applicants are **primarily collected through interviews, questionnaires and electronic tools (for biometric data), several Member States have started to use social media analysis, analysis of mobile devices and AI to collect data on asylum applicants. Data collected in the asylum procedure are mostly stored in databases,** although some Member States still use a combination of databases, electronic files and paper files. In some cases, this has led to inefficiencies and challenges in the exchange of information between asylum authorities. Member States considered increased digitalisation of data management in the asylum procedure (including the storage of data in centralised databases) as a good practice that improves data quality and speeds information transmission and access to necessary data. **Databases containing data on asylum applicants can, in most cases, be accessed by different authorities involved in the asylum procedure, easing information exchange and reducing the need to re-collect data**. In several Member States and Norway, access to specific categories of data may also be granted under some circumstances to authorities outside the asylum procedure (e.g. health authorities, labour authorities, intelligence services) for purposes other than the asylum procedure.

While most Member States and Norway cross-check data on asylum applicants against European (VIS, SIS, Eurodac) and national databases at some stage of the asylum procedure, few Member States cross-check data against international databases (e.g. Interpol SLTD). Most of the cross-checks happen during the lodging phase, although in some cases, data are cross-checked against national, European and international databases in more than one phase of the asylum procedure.

EU law requires Member States to ensure that the data protection rights of asylum applicants are guaranteed, including through the provision of information on personal data collected, data quality checks and the establishment of a data protection supervisory mechanism. Thus, **most Member States and Norway provide asylum applicants with a privacy notice** (containing information on personal data collected and processed), which is typically provided in writing and/or verbally during the lodging and/or examining phases. Whenever a privacy notice is provided, translation and interpretation is usually offered. The GDPR recognises asylum applicants' rights to access, erase and rectify their data, which, depending on the Member State, can be requested in person, electronically or by post. **In line with the exceptions contained in the GDPR, some Member States do not always allow the erasure of data (or some categories of data) related to asylum applicants.**

The majority of the Member States and Norway assess the quality of personal data collected in the asylum procedure for accuracy, timeliness, completeness,

consistency, duplication and validity. These quality checks are centralised in most Member States and generally happen throughout the phases of the asylum procedure (rather than retroactively). Several Member States have also put in place automatic quality checks. Additionally, Member States and Norway have a data protection supervisory and compliance mechanism to ensure the lawfulness of the processing of personal data in the asylum procedure. In some cases, these mechanisms are **part of the general national data protection supervision procedures entrusted to the respective national DPA, and in others, they have been established as specific mechanisms under the competence of migration authorities**.

Since 2014, most Member States have experienced challenges in data management, primarily related to the lack of human or financial resources and the interoperability of databases. Staff shortages have created capacity issues and data protection challenges in several Member States. Issues related to the interoperability of databases have sometimes led to data inconsistencies, as well as difficulties in cross-checking data, communication challenges and duplication of effort in data collection. A number of Member States also reported facing issues when cross-checking data against national, European and international databases during the asylum procedure (i.e. completeness of the data, false/inaccurate information, different rules applicable to different databases). Other challenges faced by Member States related to technical limitations in data processing (old equipment, lack of technical capacity), issues related to transliteration, and adequate implementation of the GDPR.

Several Member States and Norway have introduced changes in response to these challenges, generally aimed at increasing the digitalisation of data management, maximising the efficiency of the asylum procedure, responding to a high influx of asylum applicants, and improving the implementation of the GDPR. Several Member States introduced new databases or consolidated existing databases to mitigate the issue of interoperability and ensure smooth communication between all actors involved in the asylum procedure. Since 2014, most Member States introduced formal/informal channelling systems to accelerate or prioritise some asylum applications (applications from safe third countries of origin, vulnerable people, manifestly unfounded applications), smoothing the asylum procedure.

A number of Member States and Norway adopted contingency measures for data management (i.e. more flexibility in the different phases of the asylum procedure and contingency protocols), seeking to accelerate and ease the process in times of high numbers of asylum applicants, while also aiming to make their asylum systems crisis-proof. In 2020, the COVID-19 pandemic brought significant additional challenges that translated into changes in the asylum procedure, including the temporary suspension of registration of applications, introduction or acceleration of digitalisation of some steps of the asylum procedure (e.g. remote interviews), and changes in the collection of fingerprints.

ANNEXES

ANNEX 1. NATIONAL STATISTICS RELATED TO THE ASYLUM PROCEDURE

Table 1. Time limits in national asylum legislation in Member States and Norway - normal asylum procedures

	Making	Registering	Lodging	Examining
AT			Without delay once information collected during initial questioning is received	
BE	immediately or within eight working days of illegal entry in Belgium; or before the short stay of less than three months has ended; or within eight working days of the end of a long stay of more than three months; or immediately upon attempt to cross the Belgian border illegally	Three working days	Within 30 days after the application is made[317]	Within six months after the transfer of the file to the CGRS
CY		Within three to six working days after the application is made		
CZ		Within three working days when the application is made directly to the Ministry of the Interior. Within six working days when the application is made to the police.	Between four and seven days after registration	
DE	At the time of or immediately after entering Germany	Without delay after the application is made (in practice max. 14 days)	Within 14 days after registration	Within six months of lodgement
EE	Immediately on entering the national territory	Within three working days after the application is made		Within six months of lodgement

317 Time limit can be extended by Royal Decree in exceptional circumstances.

	Making	Registering	Lodging	Examining
ES	Immediately or within one month of entry in Spain or of events that justify a well-founded fear of persecution or serious harm	No time limit is provided for in our legislation	No time limit is provided for in our legislation	6 months normal procedure 3 months accelerated procedure 4 days border procedure
FI	Immediately on entering the national territory (or as soon as possible)	-Without delay/ Immediately after a person has made an application (at the latest within three weekdays of making the application in exceptional circumstances)		Within six months after the application is made
FR		Within three working days after the application is made	Within 21 days	Within six months of lodgement
HR	Immediately	Within three working days after the application is made	Within 15 of the registration	Within six months after the application is lodged
HU		Within three working days after the application is made		
IE	None (Ireland does not have statutory time limits in the protection procedure and does not participate in the recast Asylum Procedures Directive)	None		None
IT		Within three working days after the application is made		Examination hearing is scheduled within 33 days of the lodgement [318]
LT		Within 48 hours after the application is lodged		Examination takes place-between 7 working days and six months from the decision to examine the application
LU		Within three working days after the application is made		Within six months of the lodgement
LV		Within three working days after the application is made		
MT		Within three working days after the application is made		Within six months of the lodgement
NL		Within three working days after the application is made at an competent authority. Within six working days after the application is made at any other authority.	It is the responsibility of the applicant to lodge the application without delay	Within six months of the lodgement. This can be extended to a maximum of 18 months
PL		Within three working days after the application is made		

318 The Territorial Asylum Commission can extend the deadline up to 6 months when it is necessary to acquire further elements to take a decision and up to 9 months if the examination of the application proves to be difficult.

	Making	Registering	Lodging	Examining
PT		Within three working days after the application is made		
SI	No time limits in place			
SE	Within three working days after the application is made (making, registering and lodging are normally done at the same time)			Within six months after the application was made. The time limit to finalise an application can be extended by 9 months if exceptional circumstances apply. The entire application must be handled within six months
SK	Making, registering and lodging is entailed in one proceeding and it has be conducted in one day.			The entire application must be handled within six months
NO[319]		Within two days		First instance decision provided within 21 days

319 These time limits are not set in national legislation in Norway but are internal procedures to be followed.

ANNEX 2

Table 1. Information collected in each phase of the asylum procedure[320]

	Registration[321]	Self-registration	Lodging[322]	Examination
Personal data				
Current name	AT, BE, CY, CZ, DE, EE, ES, EL, HR, HU, FI, FR, IT, IE, LT, LU, LV, NL, PL, PT, SI, SK, SE, NO	NL	AT, CZ, CY, ES, FR, HR, HU, IT, LV, PT, SI, SE	AT, CY, HR, FR, HU, IT, SK, NO
Birth name	AT, BE, CY, CZ, DE, EL, ES, FR, HR, HU, IE, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	AT, CY, CZ, ES, FR, HR, HU, IT, LV, PT, SI, SE	AT, CY, FR, HR, HU, IT, SK, NO
Previous name	AT, CZ, DE, EE, EL, EL, ES, FI, HR, HU, LT, LU, LV, NL, PL, PT, SI, SK, SE, NO		AT, BE, CZ, ES, HR, HU, FR, IT, LV, NL, PT, SI, SE	AT, CY, FI, FR, HR, HU, IT, NL, SK, NO
Pen name	AT, CZ, DE, EE, EL, ES, FI, FR, HR, HU, LU, LV, PT, SI, SK, SE, NO		AT, BE, CZ, ES, HR, HU, FR, IT, LV, NL, PT, SI, SE	AT, CY, FI, FR, HR, HU, IT, SK, NO
Religious name	DE, EL, ES, HU, PL, SK, SE		ES, HU, IT, PT, SE	CY, HU, IT, PT, SK
Other names	AT, CY, DE,[323] EL, ES, HR, HU, IE, PL, SK, SE[324]		AT, BE, ES, CY, HR, HU, IT, SE	AT, CY, FI, HR, HU, IT, SK
Sex	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	AT, CY, CZ, ES, FR, HR, HU, IT, LV, PT, SI, SE	AT, CY, FR, HU, IT, SK
Biometric data				
Photo	AT, BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, SI, SK, SE, NO		CY, CZ, ES, FR, HR, LV, PT, SI, SE	AT, FI[325]
Fingerprints	AT, BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, SI, SK, SE, NO		CY, ES, HR,[326] LV, MT, PT, SI, SE	
Iris scan	EL			

320 If data is re-used but not re-collected in a following phase, data is not collected in that phase. Therefore, this table reports on data collected in a specific phase. LT NCP: In LT, all data presented in the table and collected in the first phase can be re-used in the examination phase. However, in some cases, the data collected in the initial phase can change in examination phase (e.g., reasons for flying, citizenship, place and date of birth, vulnerabilities) and be re-collected.
321 In the case that registration is conducted concurrently with lodging, information is included in this column.
FI: this phase or examination, BE: only in the case of unaccompanied minors, CZ, DE: not obligatory.
322 SI: lodging and/or examination; In Belgium, these data are collected during an interview that takes place at the Immigration Office shortly after the lodging of the application, but prior to examination by the CGRS
323 Artist name, monastic name, spelling of names under German law, names not defined.
324 Clan name
325 If not collected already at the registration/lodging phase.
326 in certain circumstances authority competent for lodging may collect fingerprints.

	Registration[321]	Self-registration	Lodging[322]	Examination
Other				FI [327]
Eye colour	AT, BE, DE, EL, FI, IT, LV, PL		LV,	AT
Height	AT, BE, DE, EL, FI, IT, LV, PL, SE		LV, PT	AT
Date of birth	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IT, LV, PT, SI, SE,	AT, CY, FR, HR, HU, IT, SK, NO
Citizenship(s)	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IT, LV, PT, SI, SE	AT, FR, HR, IT, SK, NO
Country of origin	AT, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	BE, CY, CZ, ES, FR, HR, HU, IT, LV, PT, SI, SE	AT, CY, HR, HU, IT, SK, NO
Place of birth				
Town	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IE, IT, LV, PT, SI, SE	AT, CY, HR, HU, FI, FR, IT, SK, NO
Region	AT,[328] CY, CZ, DE, EL, HU, LT, LV, MT, PL, PT, SI, SK, SE, NO	NL	BE, CY, CZ, HR, HU, IE, IT, LV, PT, SI, SE	AT, CY, EE, FI, HR, HU, IT, LU, SK, NO
Country	AT,[329] BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IE, IT, LV, PT, SI, SE	AT, CY, HR, HU, FR, IT, SK, NO
Other	SE, SK,[330]NO[331]		IT,[332] SE	IT,[333]SK[334]
Date of arrival in the (Member) State	AT, BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IT, LV, NL, PT, SI, SE	AT, CY, FR, HR, HU, IT, PT, SK
Last place of residence in the country of origin	AT,[335] DE, EE, EL, FI, HR, LU, LT, LV, NL, PL, SE, NO	NL	BE, CZ, ES, HR, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, EE, FR, HR, HU, IT, PT, SK, SK, NO

327 Signature
328 Collected on a voluntary basis in Austria.
329 Collected on a voluntary basis in Austria.
330 Ethnicity or tribal identity.
331 Place of arrival in the Member State.
332 Name of father and mother.
333 Name of father and mother.
334 Ethnicity or tribal identity.
335 Collected on a voluntary basis in Austria.

	Registration[321]	Self-registration	Lodging[322]	Examination
Last place of residence before entry in the (Member) State	AT[336], EE, EL, FI, HR, LT, LV, NL, SK, SE, NO	NL	BE, CZ, FR, HR, IE, IT, LV, MT, NL, PT, SE	AT, CY, EE, FR, HR, HU, IT, LU, PT, SK, NO
Contact details				
Phone number	AT,[337] CY, DE, EE, EL, FI, FR, IE, IT, LT, LU, LV, MT, PL, SE, NO		CY, FR, HR, IE,[338] IT, LV, NL, PT, SE	AT, CY, CZ, FR, HR, HU, IE,[339] PT, SK
Email address	AT[340], CY, DE, EE, EL, FI, FR, IE, IT, LT, LU, LV, SE, NO		CY, FR, IE,[341] IT, LV, NL, PT, SE	AT, CY, CZ, FR, HU, IE,[342] PT, SK, NO
Current address[343]	AT[344], BE, CY, DE, EE, EL, FR, IT, LT, LV, MT, PL, PT, SK, SE, NO		BE, CZ, FR, HR, IT, LV, PT, SK, SE	AT, BE, CZ, FI, FR, HR, HU, IE, IT, PT, SK, NO
Other	DE, NO		SE	FI, HU, NO
Civil status	AT,[345] CY, DE, EE, EL, FI, FR, HR, LT, LU, LV, SE, NO		BE, CY, CZ, FR, HR, IE, IT, LV, MT, NL, SE	AT, CY, FI, FR, HR, IT, NL, NO
Accompanied by:				
Spouse or civil partner	AT,[346] BE, CY, DE, EE, EL, FI, FR, HR, HU, LT, LU, LV, PL, PT, PT, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, IT, NL, PL, PT, SK
Children	AT,[347] BE, CY, DE, EE, EL, FI, FR, HR, HU, LT, LU, LV, PL, PT, SK, SE, NO	NL	CY, CZ, ES, FR, HR, HU, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, IT, NL, PL, PT, SK
Parents	AT,[348] BE, DE, EE, EL, FI, HR, HU, LT, LU, LV, PL, SK, SE, NO	NL	ES, FR, HR, HU, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, IT, NL, PL, PT, SK
Other relatives	AT,[349] BE, DE, EE, EL, FI, HU, LT, LV, SK, SE, NO	NL	ES, FR, HR, HU, IT, LV, MT, NL, SI, SE	AT, CY, FR, HR, HU, IT, LU, NL, SK
Family members in the (Member) State:				

336 Collected on a voluntary basis in Austria.
337 Collected on a voluntary basis in Austria.
338 In Ireland, contact details are collected at the registration phase, but can be re-collected via a change of address form at later stages.
339 In Ireland, contact details are collected at the registration phase, but can be re-collected via a change of address form at later stages.
340 Collected on a voluntary basis in Austria.
341 In Ireland, contact details are collected at the registration phase, but can be re-collected via a change of address form at later stages.
342 In Ireland, contact details are collected at the registration phase, but can be re-collected via a change of address form at later stages.
343 In Luxembourg, this information is automatically fed into the databases of the Ministry of Foreign and European Affairs via the National Registry of Physical Persons.
344 Collected on a voluntary basis in Austria.
345 Collected on a voluntary basis in Austria.
346 Collected on a voluntary basis in Austria.
347 Collected on a voluntary basis in Austria.
348 Collected on a voluntary basis in Austria.
349 Collected on a voluntary basis in Austria.

	Registration[321]	Self-registration	Lodging[322]	Examination
Name	AT,[350] CY, DE, EE, EL, FI, FR, HR, LT, LV, PL, SE, NO		BE, CY, CZ, ES, FR, HR, IE, IT, LV, MT, PT, SI, SE	AT, CY, FR, HR, HU, IT, LU, NL, PL, SK, NO
Residency	AT,[351] CY, DE, EE, EL, FR, HR, LT, LV, PL, SE, NO		BE, CY, CZ, ES, FR, HR, IE, IT, LV, MT, PT, SI, SE	AT, CY, FI, FR, HR, HU, IT, LU, NL, PL, SK, NO
Citizenship	AT,[352] CY, DE, EE, EL, FR, HR, LT, LV, PL, SE, NO		BE, CY, CZ, ES, FR, HR, IE, IT, LV, MT, PT, SI, SE	AT, CY, FI, FR, HR, HU, IT, LU, NL, PL, SK, NO
Other	AT[353], EE, LT		BE, CZ, EE, FR, IT, [354]MT, SI	AT, FR, HU, IT,[355]LU,[356]SK
Family members in another (Member) State	AT,[357] HR, EE, EL, FI, FR, LT, LV, PL, SE, NO		BE, CZ, ES, HR, IE, IT, LV, MT, PT, SI, SE	AT, CY, FR, HR, HU, IT, LU, NL, PL, SK, NO
Close relatives in the (Member) State	AT,[358] HR, EE, EL, FI, FR, LT, LV, PL, SE, NO		BE, ES, HR, IT, LV, MT, PT, SI, SE	AT, CY, FR, HR, HU, IT, LU, NL, PL, SK, NO
Close relatives in another (Member) State	AT,[359] HR, EE, EL, FI, FR, LT, LV, PL, SE, NO		BE, ES, HR, IT, LV, MT, PT, SI, SE	AT, CY, FR, HR, HU, IT, LU, NL, PL, SK, NO
Health status[360]				
Specifics on health status	BE, CY, DE, EE, EL, FI, HR, HU, FR, LT, LV, PL, SE, SK,[361] NO		BE, CZ, FR, HR, HU, IE, IT, LV, MT, PT, SI, SE	AT, BE, CZ, EE, FI, FR, HR, HU, IT, LU, NL, SK, NO
Reference that a general health check has been carried out	CY, DE, EL, FR, HR, HU, SE, SK,[362] NO		HR, HU, IT,[363] SE	FR, HR, HU, IT, NL, SK, NO
Other	DE,[364] HU, NL, SE[365], NO[366]		HU, SE	HU
Education				

350 Collected on a voluntary basis in Austria.
351 Collected on a voluntary basis in Austria.
352 Collected on a voluntary basis in Austria.
353 Collected on a voluntary basis in Austria.
354 sex, place of birth and date of birth of the family members. If the applicant has one or more CHILDREN in Italy, he/she must provide the following information: name, surname, sex, date of birth and place of birth, citizenship, residence in Italy.
355 Sex, place of birth and date of birth of the family members.
356 File number.
357 Collected on a voluntary basis in Austria.
358 Collected on a voluntary basis in Austria.
359 Collected on a voluntary basis in Austria.
360 ES: No specific questions are asked to the applicant about his/her health at any stage, without prejudice to the applicant mentioning them as a reason for his/her application or the Official taking a statement or the Instructor may ask for evidence of vulnerability of the applicant.
361 Only in case of application lodged in detention.
362 Only in case of application lodged in detention.
363 If the applicant has been in the hotspot, he/she has undergone a health check in the hotspot prior to registration/lodging.
364 Vaccination carried out during registration.
365 Medical certificates and/or vaccination certificates presented by the applicant
366 NL and NO Examination for tuberculosis.

	Registration[321]	Self-registration	Lodging[322]	Examination
School attendance	AT,[367] DE, EE, EL, LT, LV, PL, SE	NL	BE, ES, FR, HR, IT, LV, NL, PT, SI, SE	AT, CY, FI, FR, HR, HU, IT, LU, NL, PL, PT, SK, NO
Academic studies	DE, EL, LT, LV, PL, SE	NL	BE, ES FR, HR, IT, LV, MT, NL, PT, SI, SE	CY, FI, FR, HR, HU, IT, LU, NL, PL, PT, SK, NO
Trainings	DE, EL		BE, ES FR, HR, IT, SI	CY, FI, FR, HR, HU, IT, NL, PL, SK, NO
Apprenticeships	DE, EL, LT		BE, ES FR, HR, IT, SI	CY, FI, FR, HR, HU, IT, PL, SK, NO
Non-formal work experience	DE, EL		BE, ES FR, HR, IT, SI	CY, FI, FR, HR, HU, IT, PL, SK, NO
Other			ES, IT[368] LT, MT	HU, IT, PL, SK
Language skills	CY, DE, EE, EL, FI, HR, IE, LT, LU, LV, PL, SK, SE, NO		BE, CY, CZ, DE, ES HR, FR, IT, LV, MT, PT, SI, SE	CY, HR, HU, FR, IT, NL, PL, PT, SK, NO
Profession	AT,[369] DE, HR, EL, FI, LT, LV, PL, SE	NL	BE, ES HR, FR, IE, IT, LT, LV, MT, NL, PT, SI, SE	AT, CY, HR, EE, HU, FR, IT, LU, NL, PL, PT, SK, NO
Criminal record	DE, EE, EL, FR, IT, LT, LV, NL, PL, SK, NO		ES HR, IT, LV, MT, PT, SI	AT, HR, HU, FR, IT, NL, PL, PT, SK, SE, NO
Financial resources	AT, HR, EL, FI, NL, SK, SE		ES HR, IT, NL, PT, SI, SE	AT, HR, FI, HU, FR, IT, PT, SK, NO
Supporting documents				
Passport	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, LT, LU, LV, NL, PL, PT, SK, SE, NO		CZ, FR, HR, HU, IT, MT, PT, SI, SE	AT, HR, EE, FR, HU, LU, PL, SI, SK, NO
Travel document	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, LT, LU, LV, NL, PL, PT, SK, SE, NO		CZ, FR, HR, HU, IT, MT, PT, SI, SE	AT, HR, EE, FR, HU, LU, PL, SI, SK, NO
Other	AT, CZ, DE, ES, FI, HU, IE, LT, LU,[370] LV, NL, PL, SE[371], SK,[372]NO[373]		CZ, FR, HR, HU, MT, SI	AT, FR, HR, HU, LU,[374] NL, PL, SI, SK[375]

367 Collected on a voluntary basis in Austria.
368 Military service. With regard to the work activities carried out by the applicant before his arrival in Italy, the C3 Form asks to provide information about the remuneration received, the quality of the employment, the place and periods of employment.
369 Collected on a voluntary basis in Austria.
370 National identity card.
371 Driving licence, national identity card, military service book.
372 E.g. driving licence, birth certificate.
373 National identity card, birth certificate
374 National identity card.
375 E.g. driving licence, birth certificate.

	Registration[321]	Self-registration	Lodging[322]	Examination
Reasons for fleeing	AT, EE, EL, FI (briefly), IE, LT, LU, LV, NL[376],PL, SK		BE, CY, CZ, DE, ES, FR, HR, IE, IT, MT, NL, SI	AT, BE, CY, CZ, DE, EE, FI, FR, HR, HU, IE, IT, LU, MT, NL, PL, PT, SI, SK, SE, NO
Reasons for not wanting to be returned to the competent Member State as part of a Dublin procedure	EL, FI, LT, LV, PL, SE, NO		BE, DE, ES, HR, LV, SI, SE	CY, CZ, DE, EE, FI, HR, HU, FR, IT, LU, NL, PL, PT, SI, SK, NO
Previous applications	BE, CY, DE, EE, EL, FI, FR, HR, LT, LU, LV, PL, SK, SE, NO		CZ, FR, HR, IT, LV, MT, SI, SE	AT, CY, ES, HR, HU, IT, LU, NL, PL, PT, SK, SE, NO
Information on the route taken	AT, BE, CY, EE, EL, ES, FI, FR, HR, IE, LT, LV, NL, PL, SK, SE, NO	NL	BE, CZ, DE, ES, HR, IT, LV, MT, NL, SI, SE,	AT, BE, CY, DE, EE, FI, FR, HR, HU, IT, LU, NL, PL, PT, SK, SE, NO
Information on exclusion grounds	BE, CY, EE, EL, ES, FI, LV, PL, NO		BE, HR, LV, MT, SI	BE, CY, HR, EE, ES, FI, FR, HU, IE, IT, LU, MT, NL, PL, PT, SI, SK, SE, NO
Religious affiliation	AT[377], BE, CY, DE, EL, FI, LT, LU, LV, PL, NO		BE, CZ, ES, FR, HR, IE, IT, LV, MT, SI	AT, BE, CY, EE, FR, HR, HU, IT, LU, NL, PL, PT, SI, SK, SE, NO
Vulnerabilities				
Unaccompanied minor	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, LT, LU, LV, NL, PL, SK, SE, NO		CZ, FR, HR, HU, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, LU, NL, PL, PT, SK, NO
Pregnant	BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, LT, LV, NL, SK, SE, NO		CZ, ES, FR, HR, HU, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, LU, NL, PL, SK, NO
Disabilities	BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, LT, LV, NL, SK, SE, NO		CZ, ES, FR, HR, HU, IE, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, LU, NL, PL, PT, SK, NO
Elderly	BE, CY, DE, EL, ES, FR, HR, HU, IE, LT, LV, NL, SK, SE, NO		CZ, FR, HR, HU, IT, LV, MT, NL, PT, SI, SE	AT, CY, FR, HR, HU, LU, NL, PL, SK, NO
Single parent with minor child(ren)	BE, CY, DE, EE, EL, ES, FI, FR, HR, HU, LT, LV, NL, SK, SE		CZ, ES, FR, HR, HU, IE, IT, LV, MT, NL, SI, SE	AT, CY, FR, HR, HU, LU, NL, PL, PT, SK
Victims of human trafficking	BE, CY, DE, EE, EL, FI, HR, HU, IE,[378] LT, LV, NL, SK, SE		CZ, ES FR, HR, HU, IE,[379] IT, LV, MT, NL PT, SI, SE	AT, CY, EE, FR, HR, HU, IE,[380] LU, NL, PL, PT, SK, SE

376 Only if necessary for identification purposes.
377 Collected on a voluntary basis in Austria.
378 In Ireland, this is not directly asked, but it may be volunteered by the applicant and it is recorded.
379 In Ireland, this is not directly asked, but it may be volunteered by the applicant and it is recorded.
380 In Ireland, this is not directly asked, but it may be volunteered by the applicant and it is recorded.

	Registration[321]	Self-registration	Lodging[322]	Examination
Mental disorders	BE, CY, DE, EE, EL, FI, HR, HU, FR, LT, LV, NL, SK, SE		CZ, ES FR, HR, HU, IT, LV, MT, NL, PT, SI, SE	AT, CY, ES, FR, HR, HU, LU, NL, PL, PT, SK, SE
Victims of torture, physical or sexual violence (female genital mutilation)	BE, CY, DE, EE, EL, FI, HR, HU, LT, LV, PL, SK, SE		CZ, ES FR, HR, HU, IT, LV, MT, PT, SI, SE	AT, CY, EE, FR, HR, HU, IE, LU, NL, PT, SK, SE
Other	FI, PL, SK, NO[381]		IT, SI	IT, PL, SK
Other (non-exhaustive list)				
Information on military service	NL, PL, NO		HR, IT	HR, IT
Information on membership in work unions	NO			
Signature	EE		EE, HR, IT[382]	FI, HR
Legal ground for entering the country	EE, IE,		EE	
Border crossing point	EE, FI,		EE	
Reception needs	BE, IT[383]			
Intention to move to another country			IT	
Belonging to ethnic group, political, social or religious organisation	SE		HR, IT, SE	HR, SE
Date of application	LU			LU
Other Member States of the European Union or other country granted refugee or subsidiary protection status	IE			
Request to modify personal data previously provided				SI

381 Sexual orientation if stated as grounds for persecution.
382 The registration form needs to be signed by the applicant for the application to be lodged.
383 The identification of vulnerabilities that place in the identification phase, which take place even before making an application and starting the asylum procedure.

Table 2. Heatmap of information collected in each phase of the asylum procedure[384]

In which phase(s) is this information collected?			
	Registration	**Lodging**	**Examination**
Personal data			
Current name	**24**	**12**	**8**
Birth name	**22**	**12**	**8**
Previous name	**19**	**13**	**10**
Pen name	**17**	**13**	**9**
Religious name	**7**	**5**	**5**
Other names	**11**	**8**	**7**
Sex	**25**	**12**	**6**
Biometric data			
Photo	**24**	**9**	**2**
Fingerprints	**22**	**8**	
Iris scan	**1**	**0**	
Other	**0**	**0**	**1**
Eye colour	**8**	**1**	**1**
Height	**9**	**2**	**1**
Date of birth	**25**	**11**	**8**
Citizenship(s)	**25**	**11**	**6**
Country of origin	**24**	**12**	**7**
Place of birth			
Town	**23**	**12**	**9**
Region	**16**	**11**	**10**
Country	**23**	**12**	**8**

384 In the Netherlands, data are collected both through self-registration and normal registration. Data on region of birth, spouse or civil partner, children, parents, school attendance, academic studies and criminal records are only collected through self-registration.

In which phase(s) is this information collected?			
	Registration	Lodging	Examination
Other	3	2	2
Date of arrival in the (Member) State	23	12	8
Last place of residence in the country of origin	13	12	11
Last place of residence before entry in the (Member) State	11	11	11
Contact details			
Phone number	16	9	9
Email address	14	8	9
Current address	16	9	12
Other	2	1	3
Civil status	13	11	8
Accompanied by:			
Spouse or civil partner	19	14	10
Children	19	14	10
Parents	16	12	10
Other relatives	13	10	9
Family members in the (Member) State:			
Name	13	13	11
Residency	12	13	12
Citizenship	12	13	12
Other	3	7	6
Family members in another (Member) State	11	11	11
Close relatives in the (Member) State	11	9	11
Close relatives in another (Member) State	11	9	11

In which phase(s) is this information collected?			
	Registration	Lodging	Examination
Health status			
Specifics on health status	15	12	14
Reference that a general health check has been carried out	8	4	8
Other	5	2	1
Education			
School attendance	9	10	13
Academic studies	6	11	12
Trainings	2	6	10
Apprenticeships	3	6	9
Non-formal work experience	2	6	9
Other	0	4	4
Language skills	14	13	10
Profession	10	13	13
Criminal record	11	7	11
Financial resources	7	7	9
Supporting documents			
Passport	22	9	10
Travel document	22	9	10
Other	15	6	8
Resons for fleeing	11	12	21
Reasons for not wanting to be returned to the competent Member State as part of a Dublin procedure	7	6	16
Previous applications	15	8	14
Information on the route taken	17	11	16
Information on exclusion grounds	9	5	19
Religious affiliation	11	10	16

	In which phase(s) is this information collected?		
	Registration	Lodging	Examination
Vulnerabilities			
Unaccompanied minor	**21**	**11**	**11**
Pregnant	**17**	**13**	**10**
Disabilities	**16**	**13**	**11**
Elderly	**15**	**11**	**10**
Single parent with minor child(ren)	**15**	**12**	**10**
Victims of human trafficking	**14**	**13**	**13**
Mental disorders	**14**	**12**	**11**
Victims of torture, physical or sexual violence (female genital mutilation)	**13**	**11**	**12**

Table 3. Information collected in more than one phase

Data category	More in more than one phase
Personal data	AT, CY, CZ, ES HR, FR, HU, IT, NL, PT, SI, SK, NO
Sex	AT, CY, CZ, ES, HR, FR, HU, IT, PT, SI, SK
Biometric data	AT, CY, HR, FR, SI
Date of birth	AT, CY, CZ, ES, HR, FR, HU, IT, PT, SI, SK, NO
Citizenship(s)	AT, CY, CZ, ES, HR, FR, HU, IT, PT, SI, SK, NO
Country of origin	AT, CY, CZ, ES, HR, FR, HU, IT, PT, SI, SK, NO
Place of birth	AT, CY, CZ, ES, HR, FI, FR, HU, IT, PT, SI, SK, NO
Date of arrival in the (Member) State	AT, CY, ES, HR, FR, HU, IT, NL, PT, SI, SK
Last place of residence in the country of origin	AT, HR EE, IT, NL, PT, NO
Last place of residence before entry in the (Member) State	AT, HR EE, FR, IT, NL, PT, SK, NO
Contact details	AT BE, CY, HR, FR, IE, IT, PL, PT, SK, NO
Civil status	AT, CY, HR, FR, IT, NL, NO, SK
Accompanied by:	AT, CY, HR, FR, HU, IT, NL, PL, PT, SK
Family members in the (Member) State:	AT, CY, HR, FR, IT, PL, NO
Family members in another (Member) State	AT, HR, FR, PL, NO
Close relatives in the (Member) State	AT, HR, FR, PL, NO
Close relatives in another (Member) State	AT, HR, FR, NO
Health status	BE, CZ, HR, FR, HU, IT, SK, NO
Education	AT, HR, FR, IT, NL, PL, PT
Language skills	CY, DE, FR, HR, PL, PT, SK, NO
Profession	AT, HR, FR, NL, PL, PT
Criminal record	HR, FR, IT, NL, PL, PT, SK, NO
Financial resources	AT, HR, FI, IT, NL, PT, SK
Supporting documents	AT, CZ, HR, EE, FR, HU, LU, PL, PT, SI, SK, NO
Reasons for fleeing	AT, BE, CY, CZ, DE, EE, FI, FR, HR, IE, IT, LU, MT, NL, PL, SI, SK
Reasons for not wanting to be returned to the competent Member State as part of a Dublin procedure	DE, HR, PL, SI, NO
Previous applications	CY, HR, FR, IT, LU, PL, SK, NO
Information on the route taken	AT BE, CY, ES, HR, EE, FI, FR, NL, PL, SK, NO
Information on exclusion grounds	BE, HR, EE, ES, FI, MT, PL, SI, NO
Religious affiliation	AT, BE, CY, HR, FR, IT, LU, PL, SI, NO
Vulnerabilities	AT, CY, HR, ES, FR, HU, IE, LU,[385] NL, PL, PT, SE, SK, NO
Other: date of application	LU

385 Unaccompanied minors.

LIST OF ABBREVIATIONS

AI: Artificial Intelligence

BAMF: The German Federal Office for Migration and Refugees *(Bundesamt für Migration und Flüchtlinge)*

BRP: Dutch Basic Registration of Persons (*Basisregistratie Personen)*

BVID: Dutch Basic Identity Assessment Facility (*Basisvoorziening Identificatie)*

BVV: Dutch Basic Provision for Foreigners (*Basisvoorziening Vreemdelingen)*

CGRS: Belgium Office of the Commissioner General for Refugees and Stateless Persons *(Commissariat général aux réfugiés et aux apatrides)*

DPA: Data protection authority

EASO: European Asylum Support Office

ETIAS: European Travel Information and Authorisation System

GNIB: Irish Garda National Immigration Bureau

IND: Dutch Immigration and Naturalisation Service *(Immigratie- en Naturalisatiedienst)*

IOM: International Organization for Migration

KOCV: Dutch Operational Coordination Centre for Foreign Nationals *(Ketenbreed Operationeel Coördinatiecentrum Vreemdelingen)*

OFPRA: French Office for the Protection of Refugees and Stateless Persons *(Office français de protection des réfugiés et apatrides)*

PBGB: Estonian Police and Border Guard *(Politsei- ja Piirivalveamet)*

RAKS: Estonian Register of Granting International Protection (*Riiklik rahvusvahelise kaitse andmise register*)

RIC: Reception and Identification Centre.

RNPP: Luxembourg National Registry of Physical Persons *(Registre national des personnes physiques)*

GDPR: General Data Protection Regulation

SIS: Schengen Information System

UMA: Finnish Electronic Case Management System for Immigration (*Ulkomaalaisasiain sähköinen asiankäsittelyjärjestelmä*)

UNHCR: United Nations High Commissioner for Refugees

VIS: Visa Information System

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