EMN European Migration Network ESTONIA

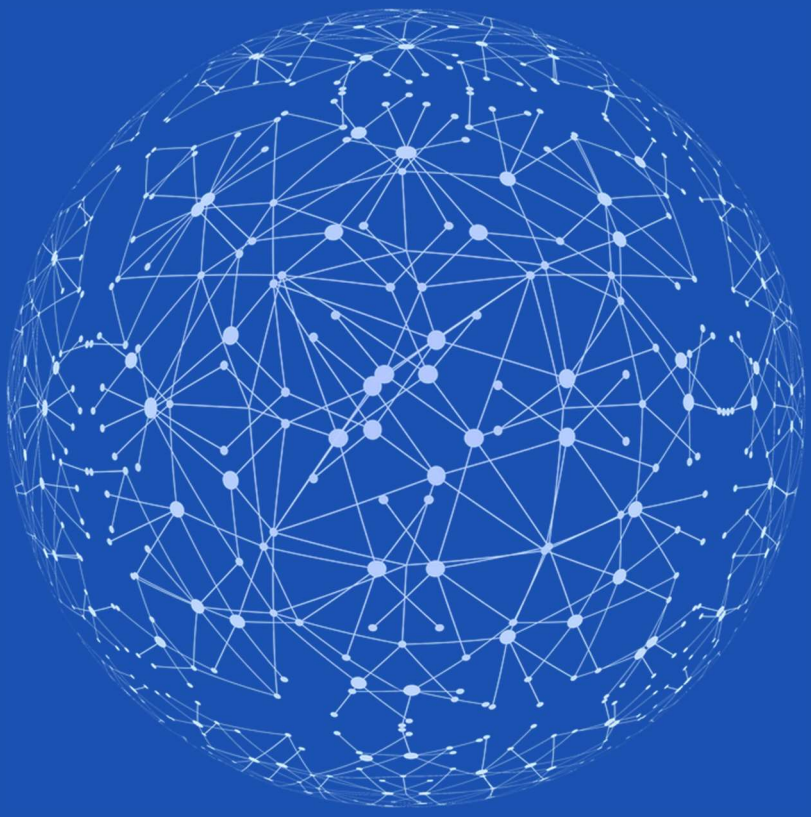
Funded by the European Union's AMIF

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

EMN Study 2020

Accurate, timely, interoperable?

Data management in the asylum procedure



Estonian National report

Disclaimer: The following responses have been provided primarily for the purpose of completing a Synthesis Report for the EMN Study on Accurate, timely, interoperable? Data management in the asylum procedure. The contributing EMN NCP have provided information that is, to the best of their knowledge, up-to-date, objective and reliable within the context and confines of this study. The information may thus not provide a complete description and may not represent the entirety of the official policy of an EMN NCPs' Member State.
This document was produced by Barbara Orloff the expert of EE EMN NCP. This report was compiled based on public and available information. Furthermore, experts of this topic were consulted.

Estonian national contact point
Estonian Academy of Security Sciences
Kase 61
12012 Tallinn
emn@sisekaitse.ee

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

Common Template for the EMN Study 2020

1 BACKGROUND AND RATIONALE FOR THE STUDY

A smooth and fast registration and identification procedure and ensuring the accuracy of the information collected, are **essential aspects of a functioning asylum procedure**. Several Member States have recently taken a wider range of measures to also improve interoperability to assist operational efficiency.[1] An **effective** asylum system relies on the collection of timely information that could appropriately channel asylum applicants into the right track, as well as on accurate and reliable information that could inform subsequent asylum decisions. Similarly, the smooth transmission of information to relevant authorities as well as the interoperability of databases where this information is collected avoid duplication and contribute to the **efficiency** of the asylum system. Finally, the use of information collected during different phases of the asylum procedure to inform further related steps of the process (including the Dublin procedure) reception conditions, and to inform future planning for the migration system (including integration and possibly return) increase the **preparedness** of the migration system overall.

Changing circumstances in asylum applications in recent years, including increases and decreases in the volume and types of applications, has led to several procedural changes in how Member States manage the asylum process. In many Member States this has also impacted on how data is collected, managed and shared throughout the process. In particular, the following policy developments have been registered.

1. In the years of high influx of asylum seekers in the EU (2015–2016) several Member States experienced major **challenges with regard to their capacities to register asylum seekers as well as with subsequent data management** across different databases within their respective asylum authorities and with regard to other authorities linked to the asylum procedure and reception of asylum applicants.[2] In several Member States there were backlogs and delays in the asylum procedure. Asylum applicants were not always able to make their application upon arrival and once their application was registered, it sometimes took months before they could finally lodge the asylum application.[3] Furthermore, multiple registrations occurred in some Member States due to a lack of interoperability of databases and a lack of technologies to digitalise the individual information and make it accessible to the different authorities. With regard to the high numbers of asylum applicants, several Member States experienced a need for automation, digitisation and innovation (such as the implementation of artificial intelligence) of various processes within the asylum procedure in order cope with the large numbers by saving resources, to limit double work, to ensure accuracy and transferability of individual information among different data systems.
2. With regard to the making, registering and lodging of an asylum application, a **trend towards shifting the collection of additional information of asylum seekers forward** (frontloading) in the asylum procedure may be observed in several EU Member States in recent years.[4] One reason is another development in several Member States, namely the introduction of channelling systems in their asylum procedures. Based on different pre-defined profiles, asylum applicants are channelled into different "first-instance procedures (prioritised procedures; accelerated procedures; border procedure; admissibility procedure".[5] In many cases, this had an impact on the asylum process as relevant information on asylum seekers needed to be collected at an earlier phase in order to allocate them to these different

[1] MPI, Chasing Efficiency: Can Operational Changes Fix European Asylum Systems? March 2020: https://www.migrationpolicy.org/sites/default/files/publications/MPIE-ChasingEfficiency-EuropeAsylum-Final.pdf
[2] EMN, Synthesis Report, Changing Influx of Asylum Seekers 2014-2016, August 2018: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_changing_influx_study_synthesis_final_en.pdf
[3] ECRE, Access to protection in Europe. The registration of asylum applications, 2018: http://www.asylumineurope.org/sites/default/files/shadow-reports/aida_accessii_registration.pdf; EMN, Annual Report on Migration and Asylum 2017, May 2018: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_annual_report_on_migration_2017_highres_en.pdf
[4] EASO, Workshop Discussion Paper, Workshop 2: Registration procedure, 9th Consultative Forum, 12th November 2019, Brussels: https://easo.europa.eu/sites/default/files/Workshop2-Discussion-Paper.pdf
[5] EASO, Workshop Discussion Paper, Workshop 3: channelling based on the profile of the applicant and the identification of special needs, 9th Consultative Forum, 12th November 2019, Brussels: https://easo.europa.eu/sites/default/files/Workshop3-Discussion-Paper.pdf

channels. In some Member States, information collection was also frontloaded for other reasons. Amongst other things, in order to shorten lengthy processing times in the asylum procedure (e.g. by limiting the need for paper and double work by digitising the collected information and implementing data quality assessments from the very beginning). A frontloaded information collection in some Member States again serves to better plan and coordinate reception facilities, estimate the need for integration and language courses for asylum seekers (e.g. number and types of courses needed in different regions) as well as other integration measures (e.g. labour market integration by asking for information on individual qualifications of the asylum seekers).

3. Last but not least, by further interlinking processes, actors and IT systems, **challenges occurred with regard to the interoperability of data systems and databases,** as well as with regard to data protection. However, several Member States introduced a range of measures to enhance interoperability on a federal and regional level or implemented larger reforms with regard to their data management, raising questions again with regard to safeguards of the individual data and 'legal' limitations of the data collection and processing mechanisms. The question of interoperability has also been discussed at EU-level in recent years with regard to the EU large scale IT systems. The Interoperability Regulation provides for future tools to enhance intra-EU data sharing and has as one of its aims to assist in the assessment of international protection applications.

Against this backdrop, the objective of this study is to examine how data is managed in the different phases of the asylum procedure and to identify any recent trends. In particular, it will (i) map Member States' data management approaches in the asylum procedure, (ii) examine whether there have been any procedural changes to enhance data sharing within the asylum authorities and beyond and how these have impacted on data management in these processes, and (iii) challenges and good practices that have arisen in relation to data management.

Scope

As for its **scope**, the study will cover different phases of the asylum procedure, beginning from the moment a person makes his or her asylum application until the first instance decision is made. It will focus, on the one hand, on data collected by various actors involved in the asylum procedure (e.g. border police registering an asylum application upon arrival; main authority for the asylum procedure; authorities responsible for unaccompanied minors etc.). On the other hand, the study will also cover data collected in the context of the asylum procedure but meant for other purposes than the asylum procedure itself (e.g. information on language skills used to better plan and coordinate integration and language courses; information on previous qualifications in order to smoothen labour market integration etcetera).

2 EU LEGAL FRAMEWORK

Directives and regulations

The functioning of the Common European Asylum System is based upon a series of EU legal instruments governing the asylum procedure. However, the management of personal data is only marginally regulated. With the exception of the **recast Eurodac Regulation (Regulation No 603/2013**, analysed below) that concerns the processing of biometric data of applicants of international protection for Dublin-related purposes, the registration of personal data in the asylum process is governed by national law. The **recast Asylum Procedures Directive (Directive 2013/32/EU)** sets out some rules in that respect, namely that the applicants must inform the competent authorities of their current place of residence and of any changes thereof as soon as possible, which suggests that this information is collected by the competent authorities. Competent authorities are also allowed to take a photograph of the applicant; however, this is not compulsory under EU law. Crucially, Article 30 of that Regulation proscribes national authorities from disclosing information regarding individual applications or the fact that an application has been made to the alleged actor(s) of persecution or serious harm.

From a privacy and personal data protection perspective, the **General Data Protection Regulation (EU) No 2016/679** is applicable to the processing of personal data in the asylum procedure. This entails the application of a series of data protection safeguards in the collection and further processing of personal data, such as the principles of lawfulness, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality. The data protection regime specific to the handling of personal data in the Eurodac system is covered in the Eurodac Regulation 603/2013.

EU centralised information systems

The abolition of internal borders in the Schengen area has required strong and reliable management of the movement of persons across the external borders, including through robust identity management. In that respect, three centralised information systems have been developed by the EU, which are currently operational: the Schengen Information System (SIS), Visa Information System (VIS) and Eurodac, all of which assist in verifying or identifying third-country nationals falling in different categories and who are on the move. SIS, VIS and Eurodac were originally envisaged to operate independently, without the possibility of interacting with one another. Progressively, the need has emerged to provide technical and legal

solutions that would enable EU information systems to complement each other. To that end, the **Interoperability Regulations 2019/817 and 2019/818** adopted on 20 May 2019 prescribe four main components to be implemented: a European Search Portal (ESP), a shared Biometric Matching Service (BMS), a Common Identity Repository (CIR) and a Multiple Identity Detector (MID). An EU agency, eu-LISA, is responsible for the operational management of these three systems.[6]

The most relevant EU information system in this regard is **Eurodac**, a biometric database storing fingerprints of applicants for international protection and irregular immigrants found on EU territory. Its primary objective is to serve the implementation of Regulation (EU) No. 604/2013 ('the Dublin Regulation'). Eurodac may also be accessed by national law enforcement authorities and Europol for the purposes of preventing, detecting and investigating terrorist offences and serious crimes. A recast proposal[7] tabled since May 2016 is currently negotiated as part of the revised Common European Asylum System (CEAS), with the aim of expanding the purpose, scope and categories of personal data stored in the system.

The **Visa Information System (VIS)** is also relevant for the purposes of the study not only in the context of further interoperability but also because it is used in the asylum procedure. The VIS processes personal data (both biographical and biometric) of short-stay (Schengen) visa applicants and to allows immigration, border control and asylum authorities to exchange such data for various purposes, including the implementation of the common EU visa policy and the assistance in the identification of the Member State responsible for an asylum claim in line with the Dublin rules. The current legal framework consists of Regulation 767/2008[8] governing the use of the system for immigration control purposes, and Council Decision 2008/633/JHA[9] on law enforcement access. A proposal is currently negotiated[10] that among other things, lowers the threshold age for fingerprinting (six years).

As for the **Schengen Information System (SIS),** it aims at ensuring a high level of security in the Schengen area by facilitating both border control and police investigations. To those ends, the SIS registers alerts on various categories of persons including third-country nationals to be refused entry or stay in the Schengen area, as well as alerts on objects, such as banknotes and identity documents. Failed asylum seekers may be registered in the SIS in accordance with the SIS rules. In 2018, the SIS legal framework was revised with a view to adding certain categories of alerts.[11]

The aforementioned information systems will be complemented in the future by three new ones that are currently under development: **the Entry/Exit System (EES)** that will register the border crossings, both at entry and exit, of all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not;[12] the **European Travel Information and Authorisation System (ETIAS)** that will enable to identify whether the presence of a visa-free traveller in the territory of the Member States would pose a security, irregular migration or high epidemic risk;[13] the **European Criminal Record Information System for third-country nationals (ECRIS-TCN)** that will enable the exchange of

[6] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, OJ L 295, 21.11.2018.
[7] COM (2016) 272final.
[8] Regulation (EC) 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13.8.2008, as amended by Regulation (EC) 810/2009, OJ L 243, 15.9.2009..
[9] Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218,13.8.2008.
[10] COM (2018) 302final.
[11] 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 L 312, 7.12.2018, p. 1–13; 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 L 312, 7.12.2018, p. 14–55; 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 L 312, 7.12.2018, p. 56–106.
[12] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017.
[13] 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, 19.9.2018.

criminal records on convicted third-country nationals and stateless persons.[14] All six information systems will be part of the interoperable data processing environment.

3 PRIMARY QUESTIONS TO BE ADDRESSED BY THE STUDY

This study will focus on the following primary questions:

- Which information is collected in the context of the asylum procedure at which point of time 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 which data protection safeguards are in place for asylum applicants during the asylum procedure?
- Which changes did Member States introduce in recent years with regard to data management in the asylum procedure and why?
- What challenges do Member States face with regard to data management in the asylum procedure, how have these been overcome, and what good practices can be shared?

The asylum procedure is divided in different phases in all Member States. First, an asylum applicant needs to make an asylum application which then needs to be registered and/or lodged by the competent authorities before the asylum interview may take place. Subsequently, a first-instance decision is made on the basis of an examination of the application. While the competent authorities responsible for the single phases may be different in some Members States, in others it may be a single competent authority covering all phases. In addition, in some Member States some of the phases mentioned above may in practice be conducted concurrently which is why there might not be the need for some Member States to differentiate between (some of) the phases. However, the asylum procedure will be subdivided into at least two phases in all Member States.

The Study will cover four main phases, based on EASO's guidance on asylum procedure:[15]

1 **Making an application:** during this phase the person expresses the intention to apply for international protection;

2 **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 the border police;

3 **Lodging an application:** the asylum application is formally lodged at the competent authority for the asylum procedure;

4 **Examination of the application.**

4 RELEVANT CASE LAW FROM THE COURT OF JUSTICE OF THE EU

CJEU, Case C-670/16 *Mengesteab*, Judgment of 26 July 2017: One of the questions referred to the CJEU involved the relationship between the two-time limits for take charge requests set out in Article 21 of the Dublin III Regulation. The Court clarified that the two months allowed to notify a Member State after a Eurodac hit may not result in a take charge request being issued more than three months after the application is lodged.

EU centralised systems have not generated any relevant case law before the CJEU in relation to their substance. However, more generally, case law on centralised storage of personal data for immigration-related purposes in the broader sense that may be relevant for the present study is the following:

- **CJEU, Opinion 1/15 of 26 July 2017:** In this case, the Grand Chamber of the CJEU evaluated the draft PNR Agreement between the EU and Canada. The Court elaborated on a series of safeguards as regards to data management, in particular: the need for clarity in specifying the scope of the data to be processed; the transfer of sensitive data requires a precise and solid justification; automated processing of personal data should take place under pre-established models and criteria that are specific and reliable; the authorities accessing the personal data are specified; any transfer of personal data to third countries must take place only if that third country ensures an essentially equivalent level of personal data protection; and the exercise of individual rights by persons whose personal data is processed is ensured.

[14] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019.
[15] Available at: https://easo.europa.eu/sites/default/files/Guidance_on_asylum_procedure_operational_standards_and_indicators_EN.pdf

- **CJEU, Case C-70/18, Staatssecretaris van Justitie en Veiligheid v A and Others, Judgment of 3 October 2019:** This case involves the processing of personal data of residence permit holders in a Dutch centralised database. The CJEU highlighted that the processing of 10 fingerprints and a facial image, besides providing a reliable way of identifying the person concerned, is not of an intimate nature and does not cause any particular physical or mental discomfort for the person concerned.

  Since the objective of the retention of data is to prevent and combat identity and document fraud, a five-year retention period establishes a satisfactory connection between the personal data to be retained and the objective pursued and thus is proportionate.

5 RELEVANT SOURCES AND LITERATURE

UNHCR

- UNHCR, Discussion Paper Fair and Fast – Accelerated and Simplified Procedures in the European Union, July 2018[16]

EU Agencies

- EASO, Practical Guidance Series, EASO Guidance on asylum procedures: operational standards and indicators, September 2019[17]
- EASO Online-Tool 'Identification of persons with special needs'(IPSN)[18]

EMN Studies

- EMN, Synthesis Report, Changing Influx of Asylum Seekers 2014-2016, August 2018[19]
- EMN, Synthesis Report, Challenges and practices for establishing the identity of third-country nationals in migration procedures, December 2017[20]

EMN Ad-Hoc Queries

- 2019.49 - Processing times first instance asylum cases. Requested on 8 April 2019.
- 2018.1348 - Member States' practice regarding the storage of photographs and fingerprints in national systems/databases. Requested on 5 December 2018
- 2018.1335 - Equipment to collect biometric data. Requested on 17 September 2018.
- 2018.1262 - Use of Cloud Services for Processing Personal Data in Immigration Cases. Requested on 17 January 2018.
- 2017.1191 - Biometric information for legal migration cases. Requested on 30 May, 2017.
- 2017.1180 - Mobile device information. Requested on 9 May, 2017

Other studies and reports

- ECRE - European Council on Refugees and Exiles, Report, Access to protection in Europe. The registration of asylum applications, Asylum Information Database (AIDA), June 2018[21]
- MPI – Migration Policy Institute, Cracked Foundation, Uncertain Future: Structural Weaknesses in the Common European Asylum System, March 2018[22]
- FRA – European Union Agency for Fundamental Rights, Biometric data in large EU IT systems in the areas of borders, visa and asylum – fundamental rights implications. Data protection, privacy and new technologies; Asylum, migration and borders[23]

[16] Available at: https://www.refworld.org/docid/5b589eef4.html
[17] Available at: https://www.easo.europa.eu/sites/default/files/2019.1882_EN.pdf
[18] Available at: https://ipsn.easo.europa.eu/european-asylum-support-office
[19] Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_changing_influx_study_synthesis_final_en.pdf
[20] Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en_v2.pdf
[21] Available at: http://asylumineurope.org/sites/default/files/shadow-reports/aida_accessii_registration.pdf
[22] Available at: https://www.migrationpolicy.org/sites/default/files/publications/CEAS-StructuralWeaknesses_Final.pdf
[23] Available at: : https://fra.europa.eu/en/publication/2015/fundamental-rights-implications-obligation-provide-fingerprints-eurodac

6 AVAILABLE STATISTICS

The following statistics are available through **Eurostat**:

Number of first-time asylum applications (lodging; migr_asyappctza) — compare with number of first-time decisions (migr_asydcfsta)

The following statistics may be available through national statistics:

Number of registrations of asylum applications

The following statistics are available through **EU databases**:

Number of lodged asylum applications

Number of Eurodac hits 2014 - 2019

Use of VIS and n of hits 2014 – 2019

Use of SIS and n of hits 2014 – 2019

7 DEFINITIONS

The following key terms are used in the Common Template. The definitions are taken from the EMN Glossary v6.0[24] unless specified otherwise in footnotes.

'Application for international protection' is defined as a request made by a third-country national or a stateless person for protection from a Member State, who can be understood to seek refugee status or subsidiary protection status, and who does not explicitly request another kind of protection, outside the scope of Directive 2011/95/EU (Recast Qualification Directive), that can be applied for separately.

'Asylum procedure': see definition for 'Procedure for international protection'.

'Beneficiary of international protection' is defined as a person who has been granted refugee status or subsidiary protection status.

'Channelling' of the asylum procedure (also 'triaging'): "The core premise of accelerated and simplified procedures is the differentiation between caseloads for their channelling into distinct case processing modalities. The triaging process is therefore the central tenet of the process. [...] Depending on the results of the analysis, claims will be channelled into appropriate case processing modalities, or as is already done in several Members States [...] into different streams or 'tracks'. Groups, as well as any specific profiles, with high and very low protection rates would be channelled into accelerated and/or simplified procedures, while other cases would be adjudicated under the regular procedure."[25]

'Country of origin' is the country or countries of nationality or, for stateless persons, of former habitual residence.

'Data management' is understood as the administrative process that includes all operations that are performed on data or on sets of data, through automated or other means, such as collection, recording, storage, retrieval, use, disclosure by transmission, dissemination or erasure. [26]

'Examination of an asylum application': see definition for 'Examination of an application for international protection'.

'Examination of an application for international protection': Any examination of, or decision or ruling concerning, an application for international protection by the competent authorities in accordance with Directive 2013/32/EU (Recast Asylum Procedures Directive) and Directive 2011/95/EU (Recast Qualification Directive) except for procedures for determining the EU Member State responsible in accordance with Regulation (EU) No 604/2013 (Dublin III Regulation).

'Lodging an asylum application': An application for international protection shall be deemed to have been lodged once a form submitted by the applicant or, where provided for in national law, an official report, has reached the competent

[24] Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/docs/interactive_glossary_6.0_final_version.pdf
[25] UNHCR, Discussion Paper F*air and Fast – Accelerated and Simplified Procedures in the European Union*, July 2018, pp. 8f. Available at: https://www.refworld.org/pdfid/5b589eef4.pdf
[26] Definition for the purposes of this study.

authorities of the Member State concerned. Member States may require that applications for international protection be lodged in person and/or at a designated place. [27]

'Making an asylum application': see definition for "Making application for international protection".

'Making application for international protection': The expression of intent to apply for international protection.

'Refugee status' is defined as the recognition by a Member State of a third-country national or a stateless person as a refugee.[28]

'Registering an asylum application': Record the applicant's intention to seek protection.[29] When a person makes an application for international protection to an authority competent under national law for registering such applications, the registration shall take place no later than three working days after the application is made. If the application for international protection is made to other authorities which are likely to receive such applications, but not competent for the registration under national law, Member States shall ensure that the registration shall take place no later than six working days after the application is made.[30]

'Procedure for international protection': Set of measures described in the Directive 2013/32/EU (Recast Asylum Procedures Directive) which encompasses all necessary steps for granting and withdrawing international protection starting with making an application for international protection to the final decision in appeals procedures.

8 TEMPLATE FOR NATIONAL REPORTS

The template provided below outlines the information that should be included in the National Contributions of EMN NCPs and Switzerland to this Study. The indicative number of pages to be covered by each section is provided in the guidance note. For national reports, the total number of pages should ideally not exceed **50 pages** (excluding the Annex). A limit of **25 pages** (excluding the Annex) will also apply to the synthesis report, in order to ensure that it remains concise and accessible.

[27] Article 6(2, 3, 4) of Directive 2013/32/EU (Recast Asylum Procedure Directive).
[28] Article 2 of Directive 2011/95/EU (Recast Qualification Directive).
[29] EASO, presentation, 9th Consultative Forum, 12th November 2019, Brussels.
[30] Article 6(1) of Directive 2013/32/EU (Recast Asylum Procedure Directive).

Common Template of EMN Study 2020

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

National Contribution from *Estonia[31]**

Disclaimer: The following information has been provided primarily for the purpose of contributing to a synthesis report for this EMN study. The EMN NCP has provided information that is, to the best of its knowledge, up-to-date, objective and reliable within the context and confines of this study. The information may thus not provide a complete description and may not represent the entirety of the official policy of the EMN NCPs' Member State.

Top-line factsheet [max. 2 pages]

*The top-line factsheet will serve as an overview of the **national reports** introducing the study and drawing out key facts and figures from across all sections, with a particular emphasis on elements that will be of relevance to (national) policy-makers.*

[31] Replace highlighted text with your **Member State** name here.

Please provide a concise summary of the main findings of Sections 0-7:

The aim of the study is to cover the different phases of asylum procedure, beginning from the moment a person makes his or her asylum application until the first instance decision is made and also to look closer what data is being collected throughout the asylum procedure. The objective of this national contribution is to examine how data is managed in the different phases of the asylum procedure in Estonia, what safeguards are in place for data protection and what challenges have arisen in relation to data management.

Asylum procedure in Estonia is following the principles of administrative proceedings provided for in the Administrative Procedure Act. The legal act regulating the asylum procedure is the Act on Granting International Protection to Alien (AGIPA). The different phases of asylum procedure are not clearly defined in the legislation as Estonia is practicing making, registering and lodging in one administrative proceeding. There is one single application form for registering and lodging. Making the application refers to the intent or indicated wish of the asylum seeker to apply for international protection. Registering an application means that the official responsible for accepting the applications registers an oral application in the Register of Granting International Protection (RAKS). Lodging the application means that the application form has been fully completed.

Regarding channelling of the asylum caseloads, there is no channelling phase or procedure as such enacted in Estonian legislation. However, there are 3 categories of cases – accelerated procedure and normal procedure and priority cases. According to the AGIPA an application shall be reviewed as soon as possible but no later than six months after the receipt of the application. The deadline can be prolonged in certain circumstances. In practice, for example in 2019 it took on average 73 days from lodging an application until first time decision was made by the Police and Border Guard Board (PBGB).

In Estonia PBGB operates as the single authority responsible and competent for all phases in the asylum process (including making, registering, lodging and examining of applications). PBGB combines the functions of border guard, police and processing of migration-related (including international protection) and citizenship applications. The main national database used for registering applications for international protection and processing the personal data of asylum seekers, is the Register of Granting International Protection (RAKS). Additionally, the information collected in the lodging and examination phase is cross-checked with various national, European and international databases. The main challenges that have emerged in cross-checking the data, are the different forms of names of the applicant and if the applicant has intentionally provided false names. Asylum applicants are provided with a privacy notice about the personal data collected from them. The information is translated to 18 languages.

There is an internal Information Security decree in force at the PBGB that regulates data processing issues. The case workers systematically check the accuracy of the data in the system. One of the preventive measures in place to get the information right is using mandatory fields. Regarding safeguards it is stipulated in the AGIPA that the proceedings concerning international protection are not public. Information containing the personal data of applicants is classified as information intended for internal use. The processing of information containing the personal data of such TCNs is permitted solely for the performance of duties prescribed by law. One of the supervision mechanisms for data protection is that there is a limited number of users in the system, and it is possible to trace by whom the information has been submitted, changed or deleted. There are system logs in place. The user must have a legal ground to process the information. Additionally, there is a data protection officer working at the PBGB who can assist the officials at PBGB in data protection matters and ensure that the rights of the data subjects are protected in accordance with the data protection legislation. Also, the information between the relevant authorities and systems is shared in encrypted form.

If the applicant for international protection wishes to access, rectify, or erase their data stored in the national database, he or she may make a request to the data protection specialist in the PBGB. They may also turn to the Data Protection Inspectorate for general advice and interpretation of the law or to make a complaint to seek protection of violated privacy rights or to make challenge to get access to Estonian public sector information after denial. Until now there have been no request made by the applicants to the PBGB regarding the data of the applicant.

Main challenges reported about data management was lack of human or financial resources, interoperability of databased and technical limitations in data processing. To solve the issues, there is a new database being developed and plans to change some of the outdated equipment.

Section 0: Impact of COVID-19

Did your (Member) State introduce any major change(s)/reform(s) related to data management due to the COVID-19 pandemic?

☐ Yes / x No

If yes, please describe these changes.

There were no major changes/reforms introduced related to data management due to the COVID-19 pandemic. At the same time practical measures were taken to protect the applicants as well as the officials of Police and Border Guard Board who were receiving asylum applications and conducting the interviews.

Personal protective equipment was used, and close contacts were avoided.

For a short period of time (about 3 weeks) the personal interviews were postponed, but the interviews continued shortly online. Also, the legal counselling service was adjusted to online or phone consultations.

At the same time the number of asylum applicants was very low with only 5 applications submitted from March to June 2020.

Section 1: The asylum procedure

Please note that the data management aspects of each phase of making, registering, lodging and examining an asylum claim will need to be described in more detail in the following Sections. This introductory section shall serve as a first overview to better understand the following sections on data management within each phase. If your (Member) State has implemented specific procedures (e.g. 'airport procedure') that deviate from the usual procedure(s), please point this out. However, (Member) States may decide on their own, into how much depth they want to go with regard to such specific or more exceptional procedures. In case (Member) States decide not to elaborate in more detail on specific procedures but focus more on their 'general asylum procedure', a reference can be made to the fact that the specific procedure will not be further elaborated in order to reduce the complexity of the study.

1.1 Overview of the asylum procedure

Please provide an overview on the regular asylum procedure in your (Member) State by answering the following questions.

1. Does your (Member) State clearly distinguish <u>in national legislation</u> among the abovementioned phases of **making**, **registering** and **lodging** of an application? (clear distinction – see the background section 7 - Definitions)

   ☐ Yes / x No

   If yes, please elaborate briefly.

   If no, please briefly describe the different phases of the asylum procedure in your (Member) State.

   Asylum procedure in Estonia is following the principles of administrative proceedings provided for in the Administrative Procedure Act. The legal act regulating the asylum procedure is the Act on Granting International Protection to Alien (AGIPA). The different phases are not clearly defined in the legislation as Estonia is practicing making, registering and lodging in one administrative proceeding. However, the maximum of 3 day deadline of registering and lodging is applied for example when the TCN has been first identified as illegally present or when there is difficulty finding a suitable interpreter.

According to Article 14 of the Act an application for international protection shall be **submitted** to the Police and Border Guard Board immediately after entering Estonia. If the TCN who is at a border checkpoint has no legal bases for entry in Estonia provided for in the Aliens Act and he or she **wishes to apply** for asylum in Estonia, he or she **shall submit** the application for international border immediately to the PBGB. Where there is a reasoned ground to believe that TCN staying in detention facilities or at border crossing points, including transit zones, at external borders, **may wish to** make an application for international protection, the Police and Border Guard Board Member States shall ensure provision of the persons with information on the possibility to do so.

According to the same Article **the registration** of an application shall take place immediately after a person has **submitted a wish** to be granted international protection but no later than three working days after the application is submitted. Where, due to an emergency, an emergency situation or a large number of applications for international protection, it is impossible in practice to respect the specified time limit, the application may be registered within ten working days as of the date of its submission.

2. a) Does your (Member) State clearly distinguish <u>in practice</u> among the abovementioned phases of **making**, **registering** and **lodging** of an application? (clear distinction – see background section 7 - Definitions)

☐ Yes / X No

If no, please briefly describe the different phases of the asylum procedure in your (Member) State specifying whether in practice some of the abovementioned phases are merged/overlapping.

In practice as well as by the law, the registering phase and lodging phase are merged. There is one single application form for registering and lodging.
Making the application refers to the intent or indicated wish of the asylum seeker to apply for international protection. **Registering an application** means that the official responsible for accepting the applications registers an oral application in the Register of Granting International Protection (RAKS). When at least the name, date of birth, citizenship, reasons for making an application and other initial data has been recorded, the application is considered as registered. The first registering of the application does not mean that the all the relevant information is submitted to the register at once, but rather that the primary data is inserted to the primary data (name, birthdate, time of expressing the wish to apply for asylum). An applicant is given the printout from the registry – a certificate of proving that an application has being accepted and a person is in Estonia legally. 3 days from the registering, the certificate in the form of the ID card of an asylum applicant is issued. Usually, all of the data required in the registering form, which is at the same time an application form, is being submitted and taken including fingerprints. **Lodging the application** means that the application form has been fully completed. The time of registering and lodging of the application are marked in the Register (two dates). Usually, the dates are identical. In other words, registering is recording basic data in the application form and lodging is completing the same form.
According to the PBGB in majority of the cases the making, registering and lodging the formal application takes place during the same day. Only in case the applicant expresses the wish to apply for asylum during night, the applicant needs medical attention or there is currently no suitable interpreter available, the lodging (that is completing the form) of the application could happen on the next day.

b) in practice, are there any differences in the division of the phases based on the different types of entry routes (i.e. land, sea, air)? For Member States implementing the **hotspot approach,** does this distinction hold in the hotspots?

In practice there are no procedural differences in making, registering and lodging the application for different types of entry routes in Estonia. The hotspot approach has not been used in Estonia.

3. a) Does 'channelling' of specific caseloads take place in the asylum procedure of your (Member) State?

   Channelling: ☐ Yes / ☐ No Yes and No

   If yes, please elaborate how the asylum procedure is organised, in relation to the single channels/tracks.

   There is no channelling phase or procedure enacted as such. However, there are 3 categories of cases – accelerated procedure and normal procedure and priority cases. Accelerated procedure is divided into the procedure where the content is being considered or not.
   According to the Article 20[2] of the AGIPA a clearly unfounded application for international protection may be reviewed under the expedited procedure, including at the border. A clearly unfounded application shall not be reviewed under the expedited procedure or the application of the expedited procedure shall be terminated if upon the application thereof it is impossible to take account of the special needs of the applicant, primarily in the case when the applicant has become a victim of torture of rape or he or she has been subjected to other serious forms of psychological, physical or sexual violence. Additionally, according to the same Article the application of an unaccompanied minor, if it is in the interest of the minor, may in certain conditions be reviewed under the expedited procedure. According to the legislation upon application of the expedited procedure the application shall be reviewed **within 30 days**. The specified time-limit may be extended where necessary in order to ensure an adequate and complete review of the application.
   There is no border procedure enacted. Usually the accelerated procedure is not done at the border.

   Additionally, the AGIPA specifies the cases when the PBGB does not review the content of the applications for international protection. According to Article 21 of the AGIPA the cases are as follows:
   1) another country may be considered as a first country of asylum for the applicant for the purposes of Article 35 of Directive 2013/32/EU;
   2) another Member State has granted international protection to the applicant and this protection is still accessible;
   3) the applicant has arrived in Estonia through a country which can be considered a safe third country;
   4) the application is subsequent and subsection 24 (4) of this Act shall be applied thereto;
   5) a dependant family member of the applicant lodges an application, after he or she consented to have his or her case be part of the proceedings of an application lodged on his or her behalf and there are no facts which would justify submission of a separate application;
   6) another country is responsible for examination of an application for international protection pursuant to Regulation (EU) No 604/2013 of the European Parliament and of the Council.

   In the cases specified above the proceedings for international protection shall be terminated by a decision to reject an application stating, inter alia, that the content of the application has not been reviewed and thereby the PBGB is not required to estimate whether the applicant complies with the requirements for the grant of international protection provided for in Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification as beneficiary of international protection.

   Additionally, according to the AGIPA[32] the Police and Border Guard Board may give priority to examining an application of an applicant with a special need and to an application the examining of which is given priority for a well-founded need.
   In practice Estonia does not use channelling of specific caseload as the overall number of applications for international protection submitted in Estonia is small and therefore there has been no practical need for channelling. At the same time the PBGB does prioritise the processing and examination of applications by children and applicants who have been detained under the Act on Granting International Protection to Aliens.[33]

[32] AGIPA Article 18 (10)
[33] PBGB

b) Did your (Member) State introduce any changes on 'channelling' since 2014?

If so, please describe the change(s) and intended purpose. If applicable and feasible, please also refer to findings of studies or evaluations on these changes made.

With the amendments to the AGIPA that came into force on 01.05.2016, the provisions of expedited procedure, clearly unfounded applications and refusal to review the applications were specified. The main aim of the amendments was to transpose the recast Asylum Procedures Directive (Directive 2013/32/EU). There were no channelling activities as such enacted.

4. a) Are there any national time frames/limits for each of the single phases (making, registering, lodging and examining a claim) in the context of Article 6 of the recast Asylum Procedures Directive?[34]

Yes / ☐ No Yes and no

If yes, please describe and specify the time frames/limits for the phases applicable in your (Member) State.

According to Article 14 of the AGIPA the application for international protection has to be submitted to the Police and Border Guard Board immediately after entering Estonia.

The same Article stipulates that the registration of an application shall take place immediately after a person has submitted a wish to be granted international protection but no later than three working days after the application is submitted. Where, due to an emergency, an emergency situation or a large number of applications for international protection, it is impossible in practice to respect the specified time limit, the application may be registered within ten working days as of the date of its submission.

To date the PBGB has not had the need to prolong the time limit according to the latter Article.

Hence, the national legislation does not stipulate a time limit for all the phases.

b) Did your (Member) State introduce any changes in the national timeframes / limits in the years since 2014?

Yes

If so, please describe the change(s) and intended purpose. If applicable and feasible, please also refer to findings of studies or evaluations on these changes made.

With the amendments to the AGIPA that came into force on 01.05.2016 a new Article was introduced to the AGIPA according to which registration of an application for international protection shall take place immediately after a person has submitted a wish to be granted international protection but no later than three working days after the application is submitted. Where, due to large number of applications for international protection, it is impossible in practice to respect the specified time limit, the application may be registered within ten working days as of the date of its submission.

The same Article was amended in 2020 adding that the application for international protection may also be registered within ten working days as of the date of its submission in case of emergency or emergency situation. The latter amendment was adopted for the implementation of the measures developed to mitigate the effects and consequences related to the pandemic spread of the coronavirus causing COVID-19 disease.

5. a) In practice, how long does the procedure take from an asylum applicant making an application to lodging the application (average days)?

According to the law and the practice of PBGB usually the making, registering and lodging an application is done on the same day. There have only been very few cases when, for example the application is submitted during the night, the registering might be done in the following day. In case the application is submitted at the border, the PBGB border officials will register the application in RAKS and the physical file will be sent to the unit responsible for the procedure of international protection.

[34] Directive 2013/32/EU (NB Denmark and Ireland do not participate in the recast Asylum Procedures Directive).

Table 1

Year	Average duration (days) from making to lodging a claim[35]
2014	In general the making of the application and lodging it is done on the same day
2015	In general the making of the application and lodging it is done on the same day
2016	In general the making of the application and lodging it is done on the same day
2017	In general the making of the application and lodging it is done on the same day
2018	In general the making of the application and lodging it is done on the same day
2019	In general the making of the application and lodging it is done on the same day

b) In practice, how long does the procedure take from lodging the application until a first instance decision is made (average days)? If information is not available, please indicate legal time limits and an indication that these are legal limits.

In case your (Member) State applies 'channelling', please specify the average time for each channel (average days; and please add additional columns in case more Channels apply). If (Member) State rather differentiates between special procedures in place (such as fast track procedures) and/or if these are interconnected with the 'channelling' please add additional columns and elaborate in a footnote what the special procedure is about – if not yet done so in Chapter 1.1)

According to the AGIPA[36] an application shall be reviewed as soon as possible but no later than six months after the receipt of the application. If pursuant to Regulation (EU) No 604/2013 of the European Parliament and of the Council Estonia is responsible for the examining of the application for international protection, the term of six months shall commence as of the moment the applicant has been surrendered to Estonia and is located in the territory of Estonia.

The time-limit may be extended by a period not exceeding nine months where at least one of the circumstances exists: 1) complex issues of fact or law are involved; 2) a large number of persons simultaneously apply for international protection; 3) the delay can be attributed to the failure of the applicant to comply with his or her obligations arising from § 11 of this Act.

By way of derogation and in duly justified circumstances, the above-mentioned time limits may be extended by three months, where it is necessary in order to ensure an adequate and complete examination of an application for international protection.

The completion of the proceedings may be postponed where the determining authority cannot reasonably be expected to take a decision within the above-mentioned time-limits due to an uncertain situation in the country of origin of the applicant, which is expected to be temporary. In such a case, the Police and Border Guard Board shall: 1) conduct assessment of the situation in that country of origin at least every six months; 2) notify the applicant within a reasonable time of the reasons for the postponement of the decision on the application; 3) notify the European Commission within a reasonable time of the postponement of proceedings of application of a person from that country of origin. In any event, an application shall be reviewed within 21 months as of the receipt of the application. If the Police and Border Guard Board cannot take a decision with regard to an application for international protection within six months as of the receipt of the application for international protection, the applicant concerned shall be informed of the delay; and upon the request of the applicant, of the reason for the delay and the time when the decision is to be expected.

The legislation[37]foresees that upon application of the expedited procedure the application shall be reviewed within 30 days. The specified time-limit may be extended where necessary in order to ensure an adequate and complete review of the application, taking account of the provisions of subsections 181 (1)–(5) of the AGIPA.

[35] In case there is no information on the exact average duration, please include estimates about the average duration.

[36] Article 181 of the AGIPA

37 AGIPA Article 20^2 (4)

As in practice Estonia does not channel applications, it is not possible to distinguish the time by channels. The following table reflects the average days from lodging an asylum application until first time decision for all the applications.

Table 2

Year	From lodging until first time decision				
	Average days	Channel 1 (please specify)	Channel 2 (please specify)	Channel 3 (please specify)	Channel 4 (please specify)
2014	100	N/A	N/A	N/A	N/A
2015	125	N/A	N/A	N/A	N/A
2016	67	N/A	N/A	N/A	N/A
2017	37	N/A	N/A	N/A	N/A
2018	57	N/A	N/A	N/A	N/A
2019	73	N/A	N/A	N/A	N/A

1.2 Authorities involved in the asylum procedure

6. Which authorities are involved in and responsible for the asylum procedure from making an application to first instance decision?

Please indicate whether those authorities are legally competent for registering an asylum application or not. For those authorities which are not, please also see Section 2.1

According to the legislation[38] the Police and Border Guard Board shall receive and resolve an application for international protection. Hence, in Estonia only the PBGB is involved and responsible for the asylum procedure. The applications are accepted by the border guard officials or migration surveillance officials depending of the place of the application. Asylum procedure, including decision making is done by the unit of international protection.

Table 3

Type of Authority	**Specify name of the authority involved in <u>making</u> an application**	**Legally competent for <u>registering</u> an asylum application (please indicate type of authority and specify name)**	**Legally competent for <u>lodging</u> an asylum application (please indicate type of authority and specify name)**	**Legally competent for <u>examining</u> an asylum application (please indicate type of authority and specify name)**
Border Police	Police and Border Guard Board, border guard or migration surveillance unit	Police and Border Guard Board, border guard or migration surveillance unit	Police and Border Guard Board, border guard or migration surveillance unit	
Local Police	Police and Border Guard Board			
(Branch) office for Refugees				
Ministries (Interior, Justice, etc.)				

38 AGIPA Article 3 (4)

Type of Authority	Specify name of the authority involved in making an application	Legally competent for registering an asylum application (please indicate type of authority and specify name)	Legally competent for lodging an asylum application (please indicate type of authority and specify name)	Legally competent for examining an asylum application (please indicate type of authority and specify name)
Local Citizen's Office/Mayor of a local city/town				
(Local) immigration office	Police and Border Guard Board		Police and Border Guard Board, international Protection Unit	Police and Border Guard Board, international Protection Unit
(Shared) accommodation for refugees				
EU Agency				
International Organisation				
Detention facility	Police and Border Guard Board			
Reception centre				
Others (please specify)				

1.3 Data collected during the asylum procedure

7. Which information is gathered during the asylum procedure at the different phases and by whom? Please, fill Table 4 below.

Table 4

1.Categories of data collected	**2. In which phase(s) is this information collected? (including self-registration)** - Registering (1) - self-registration (1.1) - lodging (2) - examination (3) *Please use the numbers provided for each phase to indicate the phase the data is collected. In case phases are combined in your state, please indicate it accordingly by using a dash (see example below).* *If data is re-used but not re-collected in a following phase, data is **not collected** in that phase. Therefore, **if data is not collected** in a specific phase but only re-used or not used at all, **please do not add any number for that phase.***	**3. Which organization collects this information in each of the different phases?** *(whenever possible please refer to the authorities listed in section 1.2*	**4. How is this particular category of data /biometric data collected?** - online self-registration - written questionnaire (in paper) - oral (interview, face-to-face) - oral (interview via phone/ videocall) - open source (e.g. social media) - analysing documents - analysing content of mobile devices (e.g. phones, laptops) - using automated or artificial intelligence for analysis of data - other: please specify (multiple answers possible) *If different data collection tools are used in the different phases, please specify it. If possible, please indicate if any specific technology is used in the process.*	**5. Where is this particular category of data /biometric data stored?** - in an electronic file - in a database - on paper	**6. If applicable, please specify the name of the database(s)**
Name					
- *current name*	1/2	Police and Border Guard Board	- oral (1/2) - written questionnaire (1/2) - analysing documents (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	Register of Granting International Protection (RAKS)
- *birth name*	-	-	-	-	-
- *previous name(s)*	1/2	*idem*	*idem*	*idem*	*idem*
- *pen name (alias)*	1/2	*idem*	*idem*	*idem*	*idem*
- *religious names*	-	-	-	-	-
- *other names*	-	-	-	-	-

Sex	1/2	*idem*	- written questionnaire (1/2) - analysing documents (1/2)	*idem*	*idem*
Biometric data					
- *photo*	1/2	Police and Border Guard Board	- electronically (a photo is taken of all applicants in the registration process of the application)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	Register of Granting International Protection (RAKS)
- *fingerprints (which fingers, rolled or pressed fingerprints)*	1/2	idem	- electronically (fingerprints are taken from all the applicants who are at least 14 years old. Both rolled and pressed fingerprints are taken.)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- EURODAC - National Fingerprint Database - RAKS (as a scanned file)
- *iris scan*	-	-	-	-	-
- *other*	-	-	-	-	-
Eye colour	-				
Height	-				
Date of birth	1/2	*idem*	- oral (1/2) - written questionnaire (1/2) - analysing documents (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
Citizenship(s)	1/2	*idem*	idem	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
Country of origin	1/2	*idem*	idem	- in the electronic file (1/2)	- RAKS

				- in a database (1/2) - on paper (1/2)	
Previous citizenship Nationality, ethnic group	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	idem
Place of birth					
- *town*	1/2	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2) - analysing documents (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *region*	3	*idem*	idem	- in the electronic file (3) - in a database (3) - on paper (3)	- RAKS
- *country*	1/2	*idem*	idem	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *other*					- RAKS
Date of arrival in the (Member) State	1/2	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2) - analysing documents (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
Last place of residence in the country of origin	1,2,3	*idem*	- oral (1/2,3) - written questionnaire (1/2)	- in the electronic file (1/2,3) - in a database (1/2,3) - on paper (1/2)	- RAKS

Last place of residence before entry in the (Member) State	1,2,3	*idem*	- oral (1/2,3) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
Contact details					
- *phone number*	1/2	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *email address*	1/2	*idem*	*idem*	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *current address*	1/2	*idem*	*idem*	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *other*					
Civil status	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
Accompanied by:					
- *spouse or civil partner*	1/2	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2) - analysing documents (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	- RAKS
- *children*	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2)	*idem*

				- in a database (1/2) - on paper (1/2)	
- *parents*	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
- *other relatives*	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Family members in the (Member) State					
- *name*	1/2	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*RAKS*
- *residency*	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
- *citizenship*	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
- *other* (place of birth, current location, international protection)	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Family members in another (Member) State	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2)	*idem*

				- in a database (1/2) - on paper (1/2)	
Close relatives in the (Member) State	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Close relatives in another (Member) State	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Health status					
- *specifics on health status*	1/2 (vulnerabilities), 3	*Police and Border Guard Board*	- oral (1/2,3) - analysing documents (medical certificate)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*RAKS*
- *reference that a general health check has been carried out*					
- *other*					
Education					
- *school attendance*	1/ 2 (question of education level is on the application for international protection)	*Police and Border Guard Board*	- oral (1/2) - written questionnaire (1/2) - analysing documents (if available)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*RAKS*
- *academic studies*	-				
- *trainings*	-				
- *apprenticeships*	-				
- *non-formal work experience*	-				

- *other*					
Language skills	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Profession	3	*idem*	- oral (3)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	
Criminal record	1/2	*idem*	- oral (1/2) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Financial resources	-				
Supporting documents					
- passport	1/2,3	*Police and Border Guard Board*	- handed in by the applicant when registering/lodging the application (1/2) -document analysis (1,2,3) - written down on list of documents handed in by applicant (1/2, 3)	- copy in the applicant's paper/electronic file and in database (1/2, 3)	RAKS
- travel document	*idem*	*idem*	*idem*	*idem*	*idem*
- other				ADD?	*idem*
Reasons for fleeing	1/2 (short version in the application), 3 (thoroughly during the interview)	*idem*	- oral (interview, face-to-face) (1/2,3) - written questionnaire (1/2)	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Reasons for not wanting to be returned to the competent Member State	3	*idem*	- oral (interview, face-to-face) (3)	- in the electronic file (3) - in a database (3)	*idem*

as part of a Dublin procedure				- on paper (3)	
Previous applications	1/2	*idem*	- oral (interview, face-to-face) (1/2) - written questionnaire (1/2) - other databases	- in the electronic file (1/2) - in a database (1/2) - on paper (1/2)	*idem*
Information on the route taken	1/2 ,3	*idem*	- oral (interview, face-to-face) (1/2,3) - written questionnaire (1/2) - analysing documents (if available)	- in the electronic file (1/2,3) - in a database (1/2,3) - on paper (1/2,3)	*idem*
Information on exclusion grounds	1/2 (involvement in armed activities or military operations), 3	*idem*	- oral (interview, face-to-face) (1/2,3) - written questionnaire (1/2)	- in the electronic file (1/2,3) - in a database (1/2,3) - on paper (1/2,3)	*idem*
Religious affiliation	3	*idem*	- oral (interview, face-to-face) (3)	- in the electronic file - in a database - on paper	*idem*
Vulnerabilities					
- Unaccompanied minor	1/2	*Police and Border Guard Board*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	RAKS
- *Pregnant*	1/2	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*
- *Disabilities (which?)*	1/2	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*

- *Elderly*	-				
- *Single parent with minor child(ren)*	1/2	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*
- *Victims of human trafficking*	1/2, 3	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*
- *Mental disorders*	1/2	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*
- *Victims of torture, physical or sexual violence (female genital mutilation)*	1/2, 3	*idem*	- oral (interview, face-to-face)	- in the electronic file - in a database - on paper	*idem*
- *other*					
- Legal ground for entering Estonia (if any) - border crossing point	1,2	*idem*	*idem*	*idem*	*idem*
Signature	1,2	*idem*	- written questionnaire (1/2)	*idem*	*idem*

8. Has your (Member) State identified any good practice in frontloading information collected by other authorities not directly connected to the asylum procedure? If yes, please elaborate and specify in which phase does the frontloading take place.

   For each good practice mentioned, please describe a) for whom it is a good practice, b) why it is considered a good practice and c) what is the source of the statement – (please indicate sources)

   In Estonia PBGB operates as the single authority responsible and competent for all phases in the asylum process (including making, registering, lodging and examining of applications). PBGB combines the functions of border guard, police and processing of migration-related (including international protection) and citizenship applications. This is a good practice since all the initial information is obtained and collected operatively by one authority and transmitted to the responsible unit within the PBGB. There is no practice in Estonia where applications for international protection have been submitted to any other authority other than PBGB.[39]

1.4 Data management during the asylum procedure

9. Please fill Table 5 based on the information given in column 6 of Table 4 (filling as many rows as the databases indicated that Table).

Table 5

Database	Overview/definition of the database (please indicate whether it is a regional, national or European database).	National authorities that have access to the databases or access to its data[40]			Data shared with other Member States (apart from the data that (Member) States share through EU databases e.g. Eurostat, VIS, SIS)	
		Name of authority/ organisation	In which phase of the asylum procedure	For what purpose	Type of data	For what purpose
Register of Granting International Protection (RAKS)	The register of granting international protection is a national database used for registering applications for international protection, process the personal data of persons applying for international protection, to manage and gather data relating to proceedings for international protection or proceedings relating to the adaptation programme conducted	1) Police and Border Guard Board (PBGB) 2) The authorized processor of the database is the Information Technology and Development Center of the Ministry of the Interior	The PBGB has access in all of the phases of the asylum procedure	The state register of granting international protection is maintained with regard to applicants for international protection, applicants for a residence permit on the basis of temporary protection, refugees, persons eligible for subsidiary protection and	-	-

[39] Interview with the PBGB official

[40] Please differentiate between access to database and access to data. 'Access to database' is understood as a national authority being authorised to have direct access to a database without the need to request data to be transmitted to them via other authorities or intermediaries. 'Access to data' is reserved to cases where an authority has access to data contained to a database, through transmission or sharing by another authority.

	on the basis of the AGIPA.			persons eligible for temporary protection, for the purpose of processing the personal data of persons who have submitted an application for international protection and for a residence permit and who have been issued a residence permit on the basis of this Act and the data relating to proceedings for international protection or proceedings for temporary protection and the data of the proceedings relating to the adaptation programme conducted on the basis of this Act.		
EURODAC	European	PBGB	When the application for international protection has been registered and when the person receives international protection.	The purpose is to determine the responsibility for examining an application for international protection by comparing fingerprints datasets.		For exchange of data with the central fingerprint database of Eurodac

Section 2: Making an asylum application

This section requests information on asylum seekers making an asylum application to an authority that is not competent to register an asylum application.

***'Making an application'**: The expression of intent to apply for international protection.*

2.1 Making an application to an authority not competent to register the asylum application

If your (Member) State does not differentiate between "making an application" and "registering an application", or if these two phases are conducted concurrently, as referred to in Section 1.1, please skip and go to Section 3.

10. What information do authorities who are not competent to register an asylum application provide to the asylum applicants on where to go and what to do?

    The authorities will direct the person who wishes to apply for asylum to the PBGB. Hence, they will provide information about the locations where to apply for asylum.

11. Do the authorities who are not competent to register any asylum application collect any data on the asylum applicant?

    ☐ Yes / X No

    If yes, please specify which type of data is collected.

    If yes, is this data further transferred to the competent authorities?

Section 3: Registering an asylum application

'Registering an asylum application': *Record the applicant's intention to seek protection.*

This section requests information on the registration of asylum applications.

If the process of registering and lodging of the asylum application are conducted concurrently (according to the law or in practice) in your (Member) State, please make this clear in Section 1 and proceed by skipping this Section and going directly to Section 4*. If however, registering and lodging of an asylum application are conducted separately in your (Member) State (e.g. in crisis times or regionally with regard to islands vs. main land, cities vs. rural areas, centralised vs decentralised) please proceed by answering the following questions in Sections 3 and 4.*

If the process of registering, lodging and examination of the asylum application are conducted concurrently (according to the law or in practice) in your (Member) State, please make this clear in Section 1 and proceed by skipping this Section and going directly to Section 5*.*

For Member States implementing ***the hotspot approach,*** *please highlight whether there are differences in the processes applied in hotspots with regard to the standard/general asylum procedure.*

3.1 Cross checking of data collected at the registration phase

12. Against which databases at i. local/regional, ii. national, iii. European and iv. international levels is the information collected during registration cross-checked[41] (please elaborate, what the purpose is of the cross-checking and if only specific categories of data are cross-checked)?

13. Does systematic cross-checking against (i) VIS and (ii) SIS take place?

    ☐ Yes / ☐ No

14. What issues has your (Member) State encountered in cross-checking data collected at registration phase?
    For each issue mentioned, please describe a) for whom it is an issue, b) why it is considered an issue and c) whether the assessment that this issue based on input from experts (please indicate sources)

3.2 Information provided to asylum applicants in the registration phase

15. Are asylum applicants provided with a processing/privacy notice[42] about the personal data collected from them during the registration phase?

[41] Purpose of cross-checking: Previous asylum applications, Prior legal residence/stay, Illegal border crossing, Illegal stay (overstay), Criminal record, Security risks, Detect counterfeit identity/travel documents, Other (please specify).

[42] The obligation to take appropriate measures to provide data subjects with a processing or privacy notice stems from Article 12 GDPR which obliges data controllers to provide "any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language." The information referred to in Articles 13 sets out the information to be provided where data has been collected from the data subject. It includes setting out the purpose of the data collected and legal basis; legitimate interests of the data controller (where this is

☐ Yes / ☐ No

If yes, please describe which information is provided (i.e. the purpose for which personal data from the asylum applicant is collected and on what basis, who has access to the information, data protection rights etc).

16. a) Who provides the information mentioned above (under Q15) (public authorities, international organisations, CSO - civil society organisations)?

    b) How is this information provided (orally, digitally, in writing or all three)?

    Please describe.

    c) Where information is provided orally, is interpretation available?

    ☐ Yes / ☐ No

    d) Where information is provided digitally, is translation available?

    ☐ Yes / ☐ No

    If yes, who provides the digital information (e.g. national authorities, NGOs etc)?

    e) Where information is provided in writing is translation available?

    ☐ Yes / ☐ No

    If yes, who provides the translation service (e.g. national authorities, NGOs etc)?

17. Is any specific training or guidance (i.e. guidelines) provided for staff responsible for data management with regard to information collected at the registration phase?

3.3 Where self-registration procedures apply, (Member) States are asked to elaborate more on the framework and experiences.

18. Does your (Member) State have any self-registration procedures in place?

    ☐ Yes / ☐ No

    If yes, please answer questions 19-23.

    If not, please move to section 4.

19. When was the self-registration procedure introduced and why?
20. Where do asylum seekers self-register (e.g. website, by phone)?
21. Are asylum seekers provided with any guidance/assistance/information on how to self-register?

    If yes, please elaborate and indicate who provides this information

22. In which languages is the self-registration procedure available?
23. Is self-registration mandatory or optional?

    Please elaborate.

used as the legal base); recipients of the data or categories of data; and if the data will be transferred to a third country or international organisation. Articles 15 to 22 refer to the data subject's rights including the rights to access, rectification and erasure; the right to object (if data is being collected for certain purposes including for a task carried out in the public interest or an official function vested in the data controller or in pursuit of legitimate interests of the data controller); right to data portability etc.

Section 4: Lodging an asylum application

This section requests information on asylum applicants lodging an asylum application.

4.1 Cross checking of data collected at the lodging phase

24. Against which databases at i. local/regional, ii. national, iii. European and iv. international levels is the information collected during the lodging phase cross-checked (please elaborate, what the purpose is of the cross-checking and if only specific categories of data are cross-checked)?

II National databases:

Criminal Records Database to receive data on previous punishments imposed for misdemeanours and criminal offences in Estonia.

Population register to check for personal data on a TCN who has been granted a residence permit or right of residence in Estonia.

Register of residence and work permits – the aim is to check for previous or current residence or work permits.

Database of TCNs staying in Estonia without legal basis (Illgeaal2) – the aim is wo check if the person has been in Estonia before without a legal basis to stay.

Border Control database (PIKO) – purpose of the database is to keep records of persons and vehicles undergoing border control ant to carry out controls in order to ensure the internal security of the state.

II National and European databases: Data is cross-checked with the Schengen Information System national register, the aim of which is to ensure security in the area of freedom, security and justice of the EU, to ensure rapid and smooth exchange of information between MS to identify persons posing a threat to public policy and public security, to identify third-country nationals refused entry, to facilitate police and judicial cooperation in criminal matters.

III European databases:

The data on fingerprints of an applicant who is at least fourteen years of age is communicated to the Central Unit of Eurodac for comparison in accordance with the Regulation (EU) No 603/2013.

VIS – database to exchange Schengen visa data.

25. Does systematic cross-checking against (a) VIS and (b) SIS take place?

☒ Yes / ☐ No

26. What issues have you encountered in cross checking data collected at the lodging phase?

For each issue mentioned, please describe a) for whom it is an issue, b) why it is considered an issue and c) whether the assessment that this issue based on input from experts - please indicate sources)

One issue that the PBGB has encountered in cross checking data collected at the lodging phase is that the name of the applicant might be inserted in different forms (especially when the applicant does not provide an identification document) and also when the applicant has falsely provided his or her name.

4.2 Information provided to asylum applicants at the lodging phase

28. Are asylum applicants provided with a processing/privacy notice[43] about the personal data collected from them during the lodging phase?

[43] The obligation to take appropriate measures to provide data subjects with a processing or privacy notice stems from Article 12 GDPR which obliges data controllers to provide "any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language." The information referred to in Articles 13 sets out the information to be provided where data has been collected from the data subject. It includes setting out the purpose of the data collected and legal basis; legitimate interests of the data controller (where this is

X Yes / ☐ No

If yes, please describe which information is provided (i.e. the purpose for which personal data from the asylum applicant is collected and on what basis, who has access to the information, data protection rights etc).

Since in practice, the phases of making, registering and lodging of asylum applications mostly takes place at the same time, it is not practical to distinguish in Estonia's case the exact timing at which the notice about the personal data collection is issued. According to PBGB, in most cases the practice is that the application is registered first and then the notice will be issued.

Processing notice may be issued in writing at the time of registering (or directly after registering) in case the applicant understands any of the 18 languages that the written notice has already been translated to. If such written translation does not yet exist, the PBGB will provide the applicant with a relevant translation within 15 days. In any case, interpreter will also provide the information verbally to the applicant.

The written notice states that the applicant for international protection has the right to the confidentiality of the data. This means, above all, that the information collected upon processing the application is kept official, it will not be given out to the applicant´s home country and the data is processed in the PBGB, accommodation centres and other authorities taking into account the personal data protection principles. The notice also declares that the applicant has the right to examine his/her data in the EURODAC electronic fingerprint database and request that incorrect data be corrected or deleted.

29. a) Who provides the information mentioned above (under Q 28) (public authorities, international organisations, CSO - civil society organisations)?

The information is provided by the officials of the PBGB as well as the councillor.

b) How is this information provided (orally, digitally, in writing or all three)?

Please describe.

The information is provided orally for all applicants and also in writing (in case a translation to a language which the applicant can understand already exists it is provided immediately, if not then within 15 days).

c) Where information is provided orally, is interpretation available?

X Yes / ☐ No

If yes, who provides the interpretation services (e.g. national authorities, NGOs etc)?

PBGB has interpreters and translators available for some languages, and for others PGBG uses the services of professional translators that are contracted by the PBGB.

d) Where information is provided digitally, is translation available?

☒ Yes / ☐ No

If yes, who provides the digital information (e.g. national authorities, NGOs etc)?

The information is digitally available on the webpage of the PBGB.

e) Where information is provided in writing is translation available?

used as the legal base); recipients of the data or categories of data; and if the data will be transferred to a third country or international organisation. Articles 15 to 22 refer to the data subject's rights including the rights to access, rectification and erasure; the right to object (if data is being collected for certain purposes including for a task carried out in the public interest or an official function vested in the data controller or in pursuit of legitimate interests of the data controller); right to data portability etc.

X Yes / ☐ No

If yes, who provides the translation service (e.g. national authorities, NGOs etc)?

The information is translated to 18 languages. The PBGB is responsible for the translation.

30. Is any specific training or guidance provided for staff responsible for data management with regard to information collected at the lodging phase?

Yes, there have been training sessions for staff responsible for data management, however, these trainings have not specifically focused only on the registration phase but all phases of asylum procedures.

Section 5: Examining an asylum application

The following sections request information on any additional data collected after an asylum application is deemed to have been lodged and before a first instance decision is issued.

5.1 Cross checking of data collected at the examination phase

31. Against which databases at i. local/regional, ii. national, iii. European and iv. international levels is the information collected during the examination phase cross-checked (please elaborate, what the purpose is of the cross-checking and if only specific categories of data are cross-checked)?

In addition to the databases mentioned in the questions about cross-checking during the registration/lodging phase, information is again collected against the following databases:

II National databases:

Criminal Records Database to receive data on previous punishments imposed for misdemeanours and criminal offences in Estonia.

Population register to check for personal data on a TCN who has been granted a residence permit or right of residence in Estonia.

Register of residence and work permits – the aim is to check for previous or current residence or work permits.

Database of TCNs staying in Estonia without legal basis (Illgeaal2) – the aim is wo check if the person has been in Estonia before without a legal basis to stay.

Border Control database (PIKO) – purpose of the database is to keep records of persons and vehicles undergoing border control ant to carry out controls in order to ensure the internal security of the state.

POLIS -

II National and European: Data is cross-checked with the Schengen Information System national register, the aim of which is to ensure security in the area of freedom, security and justice of the EU, to ensure rapid and smooth exchange of intormation between MS to identify persons posing a threat to public policy and public security, to identify third-country nationals refused entry, to facilitate police and judicial cooperation in criminal matters.

III European: VIS – database to exchange Schengen visa data.

IV Internationally: INTERPOL

32. Does systematic cross-checking against (a) VIS and (b) SIS take place?

☒ Yes / ☐ No

The verification of personal data in respect of the VIS and SIS shall be carried out already at the initial stage of the procedure when the applicant´s identification is carried out. At the examination phase the cross-checking is repeated.

33. What issues has your (Member) State encountered in cross checking data collected at the examination phase?

For each issue mentioned, please describe a) for whom it is an issue, b) why it is considered an issue and c) whether the assessment that this issue based on input from experts (please indicate sources).

The PBGB did not report of any issues in cross-checking the data collected at the examination phase.

5.2 Information provided to asylum applicants at the examination phase

34. Are asylum applicants provided with a processing/privacy note[44] about the personal data collected from them during the examination phase?

X Yes / ☐ No

35. If yes, please describe which information is provided (i.e. the purpose for which personal data from the asylum applicant is collected and on what basis, who has access to the information, data protection rights etc). a) Who provides the information mentioned above (under Q 34) (public authorities, international organisations, CSO - civil society organisations)?

In the beginning of the asylum procedure, the asylum seeker is already provided with information about the asylum procedure and his or her rights and obligations during this procedure. Additionally, the legal councilor explains to the applicant about the rights and obligations as well as the data protection rights. In the beginning of the personal interview the applicant is informed about the confidentiality clause that is binding to the PBGB officials as well as to the interpreters.

b) How is this information provided (orally, digitally, in writing or all three)?

Please describe.

The information is provided orally.

c) Where information is provided orally, is interpretation available?

X Yes / ☐ No

If yes, who provides the interpretation services (e.g. national authorities, NGOs etc)?

The PBGB is responsible for providing the interpretations services. The applicant has the right to call at his/her own expense and option, a suitable interpreter or another language mediator to accompany upon the performance of a procedural act if this is possible without delay and the objectivity of the interpretation is ensured.

d) Where information is provided digitally, is translation available?

☐ Yes / ☐ No

If yes, who provides the digital information (e.g. national authorities, NGOs etc)?

[44] The obligation to take appropriate measures to provide data subjects with a processing or privacy notice stems from Article 12 GDPR which obliges data controllers to provide "any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language." The information referred to in Articles 13 sets out the information to be provided where data has been collected from the data subject. It includes setting out the purpose of the data collected and legal basis; legitimate interests of the data controller (where this is used as the legal base); recipients of the data or categories of data; and if the data will be transferred to a third country or international organisation. Articles 15 to 22 refer to the data subject's rights including the rights to access, rectification and erasure; the right to object (if data is being collected for certain purposes including for a task carried out in the public interest or an official function vested in the data controller or in pursuit of legitimate interests of the data controller); right to data portability etc.

e) Where information is provided in writing is translation available?

X Yes / ☐ No

If yes, who provides the translation service (e.g. national authorities, NGOs etc)?

The PBGB

36. Is any specific training or guidance provided for staff responsible for data management with regard to information collected at the examination phase?

Yes, there have been training sessions for staff responsible for data management, however, these trainings have not specifically focused only on a specific phase of the asylum procedure, but on all phases of asylum procedure.

Section 6: Data quality and safeguards [max 4 pages]

The following sections request information on how data quality is managed and the safeguards that (Member) States apply.

6.1 Data quality management

37. Is the quality of (at least some categories of) data (alphanumeric and biometric) collected during the asylum procedure assessed (e.g. with regard to accuracy, timeliness, completeness, consistency, duplication and validity of the data)?

X Yes / ☐ No

There is an internal Information Security decree in force at the PBGB that regulates data processing issues.

The case workers systematically check the accuracy of the data in the system.

If yes, please elaborate on some contrasting[45] examples of data quality assessment and indicate:

a) In which phase(s) of the asylum procedure is the quality of data assessed (quality assessment)?

b) How (specific tools)[46] and by whom (centralised/decentralised) is the quality assessment carried out?

c) If decentralised, how is it ensured that the other actors get to know about data amendments and changes?

38. Do quality assessment measures only apply retroactively?

39. Are any preventative measures in place to get the information right at the very beginning? Yes/No. If yes, which safeguards are in place?

Mandatory fields.

6.2 Safeguards

40. Describe the supervision mechanism for data protection supervision of the personal data collected during the asylum procedure in your Member State.[47]

[45] It will not be feasible to elaborate on all data quality assessment measures for each type of data collected which is why we are asking for contrasting examples where different types of quality assessment measure (e.g. tools, technical equipment, data analytics etc.) apply.
[46] E.g. name transliteration, screening for duplicates against data already stored in the database, automated data quality checks, data analytics, artificial intelligence.
[47] The question does not refer to the legal framework but to how a data protection authority in a Member State supervises the implementation of that legal framework (what are the structures in place in your Member State to ensure the data subject's data protection rights are being ensured).

It is stipulated in the law[48] that the proceedings concerning international protection are not public. The PBGB, the Ministry of Social Affairs and the agencies within the area of government thereof, the detention centre, the accommodation centre for applicants for international protection, as well as the translator and other relevant persons shall maintain the confidentiality of information related to applicants and adhere to the requirements for the protection of personal data in the processing of the personal data of the said TCN. Information containing the personal data of applicants is classified as information intended for internal use. The processing of information containing the personal data of such TCNs is permitted solely for the performance of duties prescribed by law.
One of the supervision mechanism for data protection is that there is a limited number of users in the system and it is possible to trace by whom the information has been submitted, changed or deleted. There are system logs in place. The user has to have a legal ground to process the information.
There is a Data protection officer working at the PBGB who can assist the officials at PBGB in data protection matters and ensure that the rights of the data subjects are protected in accordance with the data protection legislation.
The information between the relevant authorities and systems is shared in encrypted form.

41. Have (national) data protection authorities or similar entities assessed any of the databases described above?

X Yes / ☐ No

If yes, please specify the relevant authorities, briefly describe what conclusions have they drawn, including whether such conclusions have led to changes in data management. *Please indicate sources and whether there are any published reports or audits available on these inspections..*

Yes, the Data Protection Inspectorate has assessed the PBGB in relation to Estodac (Eurodac).
The Data Protection Inspectorate has instructed the PBGB in the past to adjust the internal deadlines for storing the information related to Eurodac.

42. How is it arranged in practice the manner in which the rights of asylum applicants in relation to access, rectification and erasure of their data stored in the national systems are exercised? *Please provide available statistics concerning the number of requests made by asylum applicants, if any.*

According to the Statute of the National Register of International Protection data from the database is issued under the official request for information according to the Public Information Act or by replying to the request. Supervision on keeping the database is performed according to the Personal Data Protection Act and the Public Information Act.
The person who inserts the information to the register is responsible for the accuracy of the data. In case the responsible processor of the data discovers erroneous data or is informed about erroneous data, he or she organizes the correction of the data and adds a document to the procedural file proving the correct information or a copy of the document and makes a note to the database about the document, the time of the correction and the name of the official who made the correction.
If the applicant for international protection wishes to access, rectify or erase their data stored in the national database, he or she may make a request to the data protection specialist in the PBGB. They may also turn to the Data Protection Inspectorate for general advice and interpretation of the law or to make a complaint to seek protection of violated privacy rights or to make challenge to get access to Estonian public sector information after denial.[49]

[48] Act on Granting International Protection to Aliens Article 13
[49] https://www.aki.ee/en/guidelines/how-can-we-help-foreign-persons-and-authorities

Until now there have been no request made by the applicant to the PBGB regarding the data of the applicant.

Section 7: Responding to challenges in data management: recent reforms to the asylum procedure

7.1 Challenges and changes/reforms in data management

43. Has your (Member) State experienced any of the following challenges related to data management in the past years (since 2014)?

    Please elaborate **on each of the selected challenges**, mentioning: a) for whom it is a challenge (policy-maker, organisation, other stakeholders); b) why it is considered a challenge; and c) how was it identified as a challenge (e.g. surveys, evaluation reports, focus groups, experts opinions etc).

    X Lack of human or financial resources –

    ☐ Self-registration

    ☐ Legal obstacles

    ☐ Cooperation between national authorities

    X Interoperability of databases – According to the PBGB there is a new database being developed at the moment that would replace RAKS. The new database would have more automatic control mechanism in place.

    X Technical limitations in data processing – According to the PBGB some of the technical equipment is outdated, but there are plans to change the equipment.

    ☐ Implementation of Eurodac and/or GDPR regulation

    ☐ Lack of training/information

    ☐ Transliteration (e.g. Arabic to Latin or other alphabets)

    ☐ Other (please specify):

44. Did your (Member) State introduce any major change(s)/reform(s) related to data management in the past years (since 2014)?

    ☒ Yes / ☐ No

    If yes, please describe those changes and why they were made.

    With the General Protection Regulation, Estonia needed to align its national legislation with it and a data protection officer was appointed at the PBGB.

    If not, please move to Q48.

45. Have any of the abovementioned changes become standard operating procedure in your (Member) State?

    ☒ Yes / ☐ No

    Please elaborate

46. Were any of these changes/reforms related to data management introduced due to the introduction of 'channelling'?

    ☐ Yes / ☒ No

    If yes, please elaborate.

47. Did the reforms introduced achieve the intended results? Why?

Please elaborate and explain why the reform(s) achieved/did not achieve the intended results.
N/A

48. Would your (Member) State consider this reform (s) as a good practice?

    Please elaborate and explain why your (Member) State considers/ does not consider the reform(s) a good practice. In particular, please mention whether any of those reform(s) are believed to have improved the quality of the asylum procedure.

49. Have any on-going (unaddressed) challenges related to data management in the asylum procedure been identified in your (Member) State?

    ☐ Yes / X No

    If yes, please elaborate.

    If yes, is your (Member) State taking any steps to address these challenges?

    N/A

7.2 Contingency measures

50. Are there any contingency measures in place to accelerate and/or ease the process in times of high influx of asylum seekers with regard to data management?

    If yes, please describe those measures.

    No.

Annex 1 National statistics

Please fill in the attached excel sheet with the respective statistics for your (Member) State – provided in a separate Excel file. The Statistical Annex consists of the following:

Annex 1.1. Number of registrations of asylum applications

Number of registrations of asylum applications *Please provide the data for the years 2014-2019.*					
2014	2015	2016	2017	2018	2019
157	231	111	116	95	104

Source: Police and Border Guard Board, the data includes subsequent applications.

EMN Study_Data_manage