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

Common Template for the EMN Study 2020

Final version: 16 March 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 wide range of measures to 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

[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

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 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,

[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

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]

---

[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.

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 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:

[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.
[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, 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.
- **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]

[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

- 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]

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

Number of lodged asylum applications

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

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.

[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
[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

'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 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 ADVISORY GROUP (Core Group and Wider Group)

An 'Advisory Group' (AG) has been established within the context of this Study for the purpose of (i) developing the (common) specifications for the study, (ii) providing support to EMN NCPs during the development of the national contributions to the Study, as well as (iii) providing support to the drafting of the Synthesis Report. In addition to COM (DG HOME and JRC) and the EMN Service Provider (ICF-Odysseus), Frontex and EASO, the members of the AG for the Study include EMN NCPs from AT, BE, CY, DE, FI, HR, IE, IT, LU, NO, PL, SI, UK. Furthermore, the Migration Policy Institute (MPI) was included as an external expert.

In addition, the AG was split into a Core Group and a Wider Group, introducing a new structure of an AG within the EMN. Core Group members agreed to take more responsibility for the revision and to invest more time in all the follow-up processes (including a 2nd AG meeting). Wider Group members gave their input at the 1st AG meeting and agreed to comment on the 2nd draft of the common template before a 2nd AG meeting of the Core Group.

EMN NCPs are invited to send any requests for clarification or further information on the Study to the representatives of the Core Group.

Advisory Group (core AG members are in **bold**)

- **DE EMN NCP (Chair, Janne Grote and Anja Kuntscher)**
- **COM (Marion Finke, DG HOME)**
- COM (Anna Kadar, DG HOME)
- **COM (Martina Belmonte, DG JRC)**
- EASO (Karolina Lukaszczyk)
- **Frontex (Ilze Perczaka)**

[26] Definition for the purposes of this study.
[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).

- **AT EMN NCP (Julia Lendorfer, Martin Stiller)**
- BE NCP (Jessy Carton, Peter van Costenoble)
- CY EMN NCP (Michalis Beys)
- **IE EMN NCP** (Anne Sheridan)
- IT EMN NCP (Stefania Nasso, Francesco Giunta, Giulia Mezzetti)
- FI NCP (Tuukka Lampi)
- LU EMN NCP (Ralph Petry)
- NO EMN NCP (Stina Schulstock Holth)
- PL NCP (Patrycja Turska, Ewelina Zabardast)
- SI EMN NCP (Helena Korosec)
- UK EMN NCP (Zoe Pellatt)
- MPI (Timo Schmidt)
- **Odysseus network expert (Niovi Vavoula, Queen Mary, University of London)**
- **ICF (Nina Mavrogeorgou, Rocio Naranjo Sandalio EMN Service Provider)**

9 TIMETABLE

The following timetable is proposed for the next steps of the Study:

Date	Action
16 March 2020	Official launch of the study
3 July 2020	Submission of national reports by EMN NCPs
14 August 2020	First synthesis report (SR) to COM & AG members (1 week to provide comments)
21 August 2020	Deadline for comments (1 week to address comment and finalise)
28 August 2020	Circulation of the first SR to all NCPs (2 weeks to comment)
11 September 2020	Deadline for comments
25 September 2020	Circulation of the second draft to all NCPs (2 weeks to comment)
9 October 2020	Deadline for comments
16 October 2020	Circulation of the third (final) draft to all NCPs (2 weeks to comment)
30 October 2020	Deadline for comments
End of November 2020	Finalisation of the synthesis report, publication and dissemination

10 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.

Common Template of EMN Study 2020

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

National Contribution from *The Netherlands**[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.

General Information

In light of the amount of information in this template, a choice was made to add general information to this template in advance in a number of boxes. This is intended to make the template clearer and provide context to data management in the asylum procedure in the Netherlands.

Box 1: Stakeholders

For this study, several stakeholders have been involved that play a role in data management in the asylum procedure, comprising mainly governmental organisations. Representatives from several organisations were involved as experts for this study, i.e. the National Police, Royal Netherlands Marechaussee, Ministry of Justice and Security and the Immigration- and Naturalisation Service.

Main stakeholders
The main stakeholders in the context of datamanagement in the asylum procedure are:
- National Police;
- Royal Netherlands Marechaussee;
- Ministry of Justice and Security;
- Immigration and Naturalisation Service.

National Police (NP)
The National Police ("the Police") has the competence to supervise and to conduct identity-related investigations. As soon as there are undocumented applicants for international protection or as there is a suspicion of identity fraud, identity investigations should be conducted, which may be carried out by the Police. Within the Police, the Unit Foreign National's Identification and Human Trafficking (AVIM) is responsible for supervision of (residence of) foreign nationals, identification and registration of asylum seekers and for combating migration crime/human trafficking. The executive organisation responsible for border control within the Rotterdam harbour is the Seaport Police (ZHP).

Royal Netherlands Marechausse
The Royal Netherlands Marechaussee (Koninklijke Marechaussee, KMar) is one of the organisations that may establish identity and that handles data in the asylum procedure. The KMar is a police organisation with military status and has a wide range of tasks in the context of national and international security. It is a partner of the IND and the Police, in the sense that it has direct contact

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

with third-country nationals at the border and in other day-to-day work.[32] The tasks of the KMar include border control at airports and seaports (with the exception of the Rotterdam harbour), monitoring the internal borders with Belgium and Germany and providing assistance in asylum procedures of asylum seekers who apply for asylum directly at the border. Just as the National Police, the KMar has the competence to supervise and has the power to conduct identity-related investigations. As soon as there are undocumented applicants for international protection or as there is a suspicion of identity fraud, identity investigations should be conducted, which may be carried out by the KMar.

Ministry of Justice and Security
The Ministry of Justice and Security (which includes the Minister for Migration) is responsible for policy development on admission, stay and the return of migrants and for the organisations accountable for the implementation and execution of related legislation. The Ministry of Justice and Security is also responsible for the Protocol Identification and Labelling, which guides data management in the asylum procedure in the Netherlands.

Immigration and Naturalisation Service
The Immigration and Naturalisation Service (Immigratie- en Naturalisatiedienst, IND). is an agency of the Ministry of Justice and Security and is responsible for the implementation of Dutch immigration policy. The IND has implementing tasks in the entry, admission and supervision of third-country nationals and assesses all residence applications of people who wish to live in the Netherlands or who want to become a Dutch citizen, including applications for asylum. In this matter, the IND plays a role in the asylum procedure. The IND assesses each application individually against the rules of the policy on foreign nationals, which is realised by the Dutch parliament with consideration of (international) conventions.[33]

Other organisations
There are also other organisations involved in data management during the asylum procedure, such as the Central Agency for the Reception of Asylum Seekers (Centraal Orgaan opvang asielzoekers, COA), municipalities, the Dutch Council for Refugees (VluchtelingenWerk) and the Netherlands Admission for Identity Information (Rijksdienst voor Identiteitsgegevens). These organisations are not explained in detail in this box, due to their smaller role in data management in the asylum procedure. Wherever needed throughout the template, their role is explained. The Dutch Council for Refugees is also interviewed in the context of this study.

[32] Defence, *Taken marechaussee (Duties of the Marechaussee)* (in Dutch). For more information, please see: https://www.defensie.nl/organisatie/marechaussee/taken.
[33] Immigration and Naturalisation Service, 'What does the IND do?,' https://ind.nl/en/about-ind/Pages/What-does-the-IND-do.aspx, consulted 16 October 2020.

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. Please provide a concise summary of the main findings of Sections 1-7:*

Changing circumstances in asylum applications in recent years, including increases and decreases in the volume and types of applications, have led to several procedural changes in how Member States of the European Union 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, Member States have expressed challenges with capacities to register asylum seekers and with regard to the interoperability of data systems and databases, as well as a trend towards shifting the collection of additional information of asylum seekers forward.

Within this context, the aim of this study is to identify how data is managed in the asylum procedure in the Netherlands, focusing in particular on the collection of data, data sharing between asylum authorities, and safeguarding quality. In addition, it aims to identify challenges and good practices in relation to data management in the asylum process.

This study was conducted between March and November 2020 by EMN Netherlands in cooperation with a focus group consisting of experts from the Ministry of Justice and Security, the Immigration and Naturalisation Service, the Royal Netherlands Marechaussee (KMar), the National Police and the Research and Documentation Centre (WODC) of the Ministry of Justice and Security. The first step of this research consisted of desk research, during which reports, evaluations, guidelines and parliamentary documents were examined. In addition, interviews were held with experts from the above-mentioned organisations as well as with experts from the Dutch Council for Refugees and input was sought from the Central Agency for the Reception of Asylum Seekers (COA).

Data collection

Data management in the asylum process is decentralized in the Netherlands, meaning that different information is collected by different organisations throughout the asylum process. There are several measures in place to avoid duplication or deviation of data. Firstly, all asylum seekers undergo identification at the Basic Facility for Identity Establishment (BVID) Kiosk, conducted by the Police or the KMar. At this point, multiple databases are consulted to check for existing registrations. If no existing files are found, the asylum seeker is assigned a V-number and registered in the Central Shared Database with Basic Information on Applicants (BVV). The BVV can be accessed by all governmental organisations cooperating in the asylum process through their organisations' respective systems.

Challenge

With regard to the registration phase, experts mentioned the dependency on other organisations in case of technical issues with databases. Furthermore, as data are routinely scanned for duplication, "hits" with existing files often bring a need for further investigation, which can be cumbersome if the file is outdated or when the relation between files is unclear.

Good practice

Duplication of files is prevented due to the use of biometrics (fingerprints).
The V-number, which is connected to biometric data, is the key in exchange of data. The V-number is known by the asylum seeker and is used in all correspondence related to the asylum procedure.

Data exchange

Different organisations are authorized to amend data in the BVV depending on the situation. Data changes in the BVV are visible for partner organisations, and users are asked to specify the reason for an amendment. Furthermore, cooperating organisations can "subscribe" to a certain file so that they are notified when a change has been made.

Besides the BVV the Netherlands has its Municipal Personal Records Database (BRP) for all residents of the Netherlands, including third-country nationals. In the BRP, biographic data is registered. When a third-country national's personal data is registered in the BRP, a message is sent to the IND and a link with the V-number is established in the BVV. From the moment the administration number and the Citizen Service Number(BSN) are known in the BVV, changes in the BRP are automatically processed among organisations cooperating in the immigration process.

Data quality

Challenges

Experts of the Ministry of Security and Justice voiced the concern that, as a result of new EU rules on interoperability of databases, national authorities will be more frequently tasked with investigating data. They furthermore noted a lack of clarity on how to investigate "hits" in these databases, as some use biometrical and others biographical data to establish connections.

Good practice

As of 2017, asylum seekers can be registered in the BRP at an earlier stage. Through registration in the BRP, Asylum seekers are more likely to quickly receive a citizen service number (BSN), so that they can arrange a bank account and government services sooner.

There are several ways in which data quality is safeguarded in the asylum procedure, including through screening for duplicates upon registration and weekly sample checks by senior caseworkers. In addition, only specially authorized personnel are allowed to amend databases, and special training is provided to staff involved in data management in the asylum process. Furthermore, protocols for safeguarding of data quality have been developed and databases are designed to avoid data gaps (i.e. by making it mandatory to fill in certain fields), thus preventing errors. Moreover, through the BVID Kiosk identity-related data (including biometric data) is registered at the forefront of the asylum process. This prevents the need for registering identity-related data multiple times. Lastly, there is also a platform for ID-experts to discuss any issues regarding data (Ketenplatform Identiteit).

Challenge

In recent years, concerns related to human resources (capacity, expertise) have repeatedly been voiced by the organizations cooperating in the immigration procedure, leading to a decrease in data quality and increase in work pressure. These challenges have been addressed through hiring new staff and conducting specialized trainings, as well as through staff briefings and issuing detailed process descriptions.

Good practice

In addition to the BVID Kiosk, the renewed identification and registration procedure – which has been tested since 2018 – focuses even more on registration at the very beginning, including through the so-called "Vestibule" where objects that may assist in the establishment of the identity (e.g. identity documents, data carriers) are checked upon registration at the BVID Kiosk. This development was identified as a good practice by experts for ensuring a swift and high-quality identification and registration.

Data protection

In the Netherlands, the Dutch Immigrant Act regulates the use of personal data and biometrics in detail. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data. The tasks and powers of the Dutch DPA are described in the General Data Protection Regulation (GDPR), supplemented by the Dutch Implementation Act of the GDPR.

The Migration Coordination Department of the Ministry of Security and Justice employs an independent data protection official (Functionaris Gegevensbescherming, FG), which supervises the application of and compliance with the GDPR in as far as it concerns the facilities for which they are responsible (such as BVV and SIGMA). The organisations that fall under the Ministry of Security and Justice all have in addition to the supervising FG their own Privacy Officer that is specialized in the GDPR and/or Data Protection Act related to their own organization. Furthermore, all systems used by the IND have undergone a Data Protection Implementation Assessment (DPIA), including INDiGO. DPIA's have also been carried out on the BVV, SIGMA and Eurodac, and internal audits have been carried out by the Police on the PSH-V database.

There are arrangements making sure that asylum seekers can access their data. They can furthermore request to modify or erase data. However, erasure is limited to some extent by the Dutch Archive Law.

Challenges

Several challenges were raised regarding data protection. Ensuring knowledge on privacy among IND employees was noted as an on-going challenge, which has been addressed through awareness-raising campaigns and by installing privacy liaisons within all directorates of the IND. Furthermore experts from the KMar noted that differences in interpretation of the GDPR may arise among organizations cooperating in the asylum process. Finally, experts from the Dutch Council for Refugees found the GDPR has decreased the willingness to share information even where it is necessary for the asylum procedure, leading to delays.

Section 0: Impact of COVID-19

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

   X Yes / ☐ No

   If yes, please describe these changes.

Yes, the Netherlands did introduce temporary change(s)/reform(s) related to data management due to the COVID-19 pandemic. Additionally, there are several change(s)/reform(s) which are worth mentioning in regard to the asylum procedure and to understand the general impact of COVID-19 on the Dutch asylum procedure. Please see below.

General developments in regards to the asylum procedure in the Netherlands

- 15-3-2020 – 12-5-2020
  The application center in Ter Apel was closed. Within the restrictions of COVID-19 measures the normal application procedure was restarted on 12 May and applicants are received in the application centers in Ter Apel or Budel.[34]
- 15-3-2020 – 23-4-2020
  The registration interviews for asylum seekers were postponed.
- 15-3-2020 – 20-3-2020
  Between the closing of the application center in Ter Apel and the opening of the emergency shelter a sober alternative shelter is provided for new applicants.
- 15-3-2020 – ongoing
  When asylum seekers come to the Netherlands, they receive a medical intake and the overall health status is examined. In addition, asylum seekers from countries at risk of tuberculosis are subjected to a check for TBC. These are precautions that are always taken. As extra precautions in response to the pandemic, the temperature of all new asylum seekers is measured and the medical questionnaire has been expanded to include questions about respiratory complaints. If there is a suspicion of contamination, further medical examination will take place.[35]
- 20-3-2020 – 12-5-2020
  In Zoutkamp (location in the province of Groningen) an emergency shelter has been provided at a military base. Restrictions are in place to curb movements. This shelter is for all asylum applicants, though most Unaccompanied Minors are placed in accommodation provided by Nidos (guardian organisation).
- 20-3-2020 – ongoing
  Asylum applicants whose application has been rejected and who should leave there accommodation are allowed to stay in the reception facility.
- 23-4-2020 – ongoing
  In April, the IND has started to carry out the interviews by phone/teleconferencing, instead of carrying out the interviews in person. Though in most cases interviews in person are carried out with extra precautions taken.[36]
  1-6-2020 – ongoing
- As a mask is mandatory in public transportation if an applicant asks for asyslum at a police station, not only a train ticket is provided but also a mask.[37]

[34] *Parliamentary Papers II, 2019-2020, 2860322, 200515*
[35] For more information, please see: https://www.coa.nl/nl/actueel/nieuws/coa-bereidt-zich-voor-op-coronavirus-covid-19
[36] Interview with an expert from the Immigration- and Naturalisation Service on 30 April 2020 and additional input on 26 November 2020
[37] Kompol (site of the Dutch Police) checked on 5-11-2020

Developments in regards to data management in the Netherlands due to COVID-19

- 15-3-2020 – 12-5-2020
  The application center in Ter Apel is closed, only the most important steps of the registration process take place (this is called pre-registration): Short intake, biometrics, V-number is assigned, relevant documents are taken, luggage is checked and the relevant systems are checked (as these checks are connected to the BIVD kiosk). But first applicants for asylum are medical tested. The asylum application is not lodged as the application form (M35-H) is not signed38. However, data has been collected and processed as usual.[39]
- 15-3-2020 - ongoing
  The National Police has taken measures to maintain 1.5 meter distance when registering an asylum seeker at the BVID kiosk (which takes fingerprints, et cetera) at police stations or upon arrival at the application center Ter Apel.[40]
  Screens are placed at all necessary places and disinfectant material is available for use. The police is working according to the directives given by the Dutch government to combat COVID-19.[41]
- 15-3-2020 – 1-7-2020
  Dublin procedures are on hold, though the administrative process is continued.
- 23-4-2020 – ongoing
  Asylum applications can be lodged again during the registration process.
- 23-4-2020 – 12-5-2020
  A start is made to move applicants who stayed in the emergency shelter in Zoutkamp and who have no symptoms to regular reception locations. First they are brought to the application centers in either Ter Apel or Budel to finish the registration process and lodge there application.
  All new applicants are registered in Ter Apel, they can sign their asylum application before they are transported to Zoutkamp. Here they will stay till they can return to the application center to finish the registration process. This is to contain the potential health risks and protect the procedures at the application center.[42]
- In the Parliamentary Papers II, 2019-2020, 19 637/25 295, 2633, 9-6-2020 it is stated that the identification and registration process is fully operational. In those cases where the asylum procedure was postponed the first registration date is considered the lodging date of the asylum application and not the date the application is signed. Also it is mentioned that to limit contact moments and travel the IND has started with interviewing applicants by video call.

[38] *Parliamentary Papers II, 2019-2020, 2866252, 200320*
[39] Interview with expert from the Immigration- and Naturalisation Service on 30 April 2020
[40] Interview with experts from the National Police on 23 April 2020
[41] This information was provided by the expert of the National Police on 23 November 2020
[42] *Parliamentary Papers II, 2019-2020, 2894782, 200423 and Parliamentary Papers II, 2019-2020 35 300 VI, 127, 15-5-2020*

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.

Box 2: Explanation on asylum procedures in the Netherlands

Besides the general asylum procedure, in the Netherlands there are a few special procedures which deviate more or less from this general procedure. These special procedures are for instance applying for asylum in detention or applying for asylum when entering the Schengen area via the Netherlands (international airport or sea harbour). There is also a slightly different procedure for repeated applications.

The repeated applications are out of scope for this study, this procedure takes place after (at least) a first decision is made. In addition, in a repeated procedure the data from the earlier procedure is used, only to be amended or extended when the applicant produces any proof to justify this.

The special procedures cover only a few percent of the total influx (in 2019: detention 1%, border 4%)[43]. Although there might be some differences from a data management point, these are slight and the general asylum procedure gives a good reference on this topic. Specifying the differences that might occur in the special procedures could cloud the overall picture Therefore EMN Netherlands will answer the questions in the template for the general asylum procedure only, unless specified otherwise .

The general asylum procedure starts the moment an applicant indicates he or she wants to apply for asylum. And involves the National Police (Unit Foreign National's Identification and Human Trafficking (AVIM), the Royal Netherlands Marechaussee (KMar), the Immigration and Naturalisation Service (IND) for making, registration, lodging and examining (only IND) an application and the Central Agency for the Reception of Asylum Seekers (COA) accommodating the asylum applicants.

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)

   X Yes / ☐ No

   If yes, please elaborate briefly.

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

Yes, Dutch national legislation distinguishes between those phases. In July 2015 Dutch immigration law was adjusted to implement Directive 2013/32/EU. The Immigrant Decree (an Order in Council) was expanded with articles to describe the phases of making, registering and lodging an application (art. 3.107b and 3.108 Vreemdelingenbesluit). [44]

[43] Written input received from the IND Business Information Centre on 14 May 2020.
[44] For more information see: https://wetten.overheid.nl/BWBR0011825/2020-03-01

2. a) Does your (Member) State clearly distinguish in practice 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.

No, in the Netherlands the different phases of the asylum procedure (making, registration, lodging and examining an application) are not always clear to distinguish. Most parts are merged together in the Identification and Registration process. (So in section 3 we have only answered the questions about self-registration as we have self-registration as part of the registration process. All other questions regarding the registration process are answered in section 4, while registering and lodging of the application are merged).

When an asylum seeker reports at the Immigration Police somewhere in the Netherlands, in most cases he can apply for asylum **(make an application)** and will receive a train ticket to the Application Centre. At some of the larger police stations it is possible to **register** at the same time. In these cases the identification process is also started[45].

Asylum seekers who first come into contact with the Royal Netherlands Marechaussee are always **identified, registered** and asked to **lodge** their application before they are escorted to the Application Centre at Schiphol (mainly Schengen Border procedure, but with increased numbers also used for the general procedure) or given transport to the Application Centre in Ter Apel[46].

At the Application Centre the **registration** phase will be finished and the application is lodged if the form was not signed at a police station (or in case of large groups at the brigade of the Royal Netherlands Marechaussee).

It is also possible for an asylum seeker to report directly at the Application Centre. The phases of **making, registering** and **lodging** an application are all executed at the Application Centre and are so closely related, that in fact it is difficult to distinguish between these phases. The signing of the application form (M35) is part of the **registration** process, by signing this form the application is **lodged**.

The **examination** phase in the Netherlands starts when the rest period (*rust en voorbereidingstijd*) ends, except when the rest period does not apply (e.g. for repeat applications).

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?

No. The applicable phases (making, registering and lodging) of an application are essentially the same, although the operational details may be slightly different.

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

Channelling: X Yes / ☐ No

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

[45] Interview with experts of the National Police on 23 April 2020
[46] Interview with experts of the Royal Netherlands Marechaussee 21 April 2020

Yes, channelling takes place in the Netherlands.

The purpose of the multi-channel policy is to structure the asylum procedure as efficiently as possible. Different procedures (channels) are used for different target groups within the multi-channel policy. By implementing certain changes to the procedures within these channels, the asylum procedure can take place in a more efficient manner. The Immigration and Naturalisation Service (IND) determines at an early stage (registration phase) which procedure (channel) will be followed for the asylum application.
The channels 3 and 5 are currently 'inactive'. These channels can be activated by the Minister for Migration for a certain period in cases of extreme high influx of asylum seekers and so avoid too big backlogs. This has not been necessary yet. Every channel continues to be sufficiently safeguarded. In concrete terms, the multi-channel policy consists of the following five tracks:

Channel 1: Dublin Procedure
This channel is intended for asylum seekers who have or should have applied for asylum in another EU Member State, for example, if they have entered the Dublin-regulated territory via that Member State. In such a case, the other Member State is responsible for handling the asylum application.

Channel 2: Safe country of origin or legal stay in another EU Member State
Asylum applications are handled in this track if the applicant originates from a safe country of origin or if he/she has international protection in another Member State. The Minister for Migration determines which country may be designated as a safe country of origin.

Channel 3: Evident decisions to grant an application
Asylum applications from people who are evidently eligible for a residence permit may have their applications granted in this accelerated channel. This channel has not yet entered into force.

Channel 4: General Asylum Procedure
In this channel, all asylum applications are handled that cannot be handled in another channel. Within this channel, the standard asylum procedure is followed.

Channel 5: Evident decision to grant an application after brief investigation
If an asylum application is evidently promising, but a brief investigation is needed into, for example nationality, the application ends up in this channel. This channel has not yet entered into force.[47]

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.

The above mentioned channels were introduced in March 2016. There have been no changes since.

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?[48]

X Yes / ☐ No

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

When an asylum seeker makes an application for international protection with an official charged with

[47] EMN (2016). Annual Policy Report. Migration and Asylum in the Netherlands. p.36-38.
[48] Directive 2013/32/EU (NB Denmark and Ireland do not participate in the recast Asylum Procedures Directive).

border surveillance or with the supervision of foreign nationals, the registration has to take place within three working days after the application is made; when the application is made to another authority, registration must take place within six working days after the application was made.[49]
It is the responsibility of the applicant to lodge the application without delay[50]. The application form(M35) is signed during the registration process. By signing the form the application is lodged.
The statutory decision period for deciding on an asylum application in the General Asylum Procedure is a maximum of 6 months. Under certain circumstances, the statutory decision period can be extended to a maximum of 18 months. [51]

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

Yes. The article which states the timeframes for registering an application was first introduced in July 2015.
The article about the timeframe for examining the application was adapted in July 2015. As a result the possibilities for extension of the statutory decision period were extended.
The intended purpose of the introduction of these new articles in relation to the timeframes is to implement the Directive 2013/32/EU in the Dutch legislation[52]

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

Table 1

Year	Average duration (days) from making to lodging a claim[53]
2014	N/A
2015	N/A
2016	N/A
2017	N/A
2018	N/A
2019	N/A

For the Netherlands these data are not available. Registering the applications (as far as executed, see question 2) is done by the National Police and the Royal Netherlands Marechaussee in their own data systems. The making of a claim is in most cases not registered. An overview of all lodgings of applications is only available at the Immigration and Naturalisation service. Until now these sources have not been combined to map and analyse the asked data. But in general there are only 1-2 days between the first contact with the Dutch authorities, the registration process at the application centre and the lodging of the application. Lodging/registration occurs on day 1 and the registration interview is held on day 3.

[49] Article 3.107b Vreemdelingenbesluit (Immigration Decree). For more information see: https://wetten.overheid.nl/BWBR0011825/2020-03-01#Hoofdstuk3_Afdeling5_Paragraaf2
[50] Article 3.108c, Immigration Decree (Vb) 2000. For more information see: https://wetten.overheid.nl/BWBR0011825/2020-03-01#Hoofdstuk3_Afdeling5_Paragraaf2
[51] Article 42 Vreemdelingenwet (Immigration Act). For more information see: https://wetten.overheid.nl/BWBR0011823/2020-05-14#Hoofdstuk3_Afdeling4
[52] EMN Annual Policy Report Migration and Asylum Netherlands 2015 (p.36)
[53] In case there is no information on the exact average duration, please include estimates about the average duration.

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)

Table 1[54]

Year	From lodging until first decision			
	Average days	Channel 1 (Dublin procedure)	Channel 2 (Safe country)	Channel 4 (General procedure)
2014	118	N/A	N/A	N/A
2015	185	N/A	N/A	N/A
2016	150	99	24	231
2017	111	85	21	156
2018	172	99	26	267
2019	103	97	27	174

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

Table 2

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)
Border Police	Royal Netherlands Marechaussee National Police (only responsible for the Sea Port in Rotterdam)	Royal Netherlands Marechaussee National Police	Royal Netherlands Marechaussee National Police	-- --
Local Police	National Police)	National Police	National Police	--
(Branch) office for Refugees	--	--	--	--
Ministries (Interior, Justice, etc.)	--	--	--	--
Local Citizen's Office/Mayor of a	--	--	--	--

[54] Written input provided by IND Business Information Centre on 14 May 2020. For 2014 and 2015, the average days per channel are not provided, as the current multi-channel policy was introduced in 2016 (see response to question 3b).

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 city/town				
(Local) immigration office	--	--	--	Immigration and Naturalisation Service
(Shared) accommodation for refugees	--	--	--	--
EU Agency	--	--	--	--
International Organisation	--	--	--	--
Detention facility	--	--	--	--
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.

Please note that for categories of data which are <u>not</u> collected during the asylum procedure, the table is left empty.

Table 3

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, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (IND) (1.1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	- In databases	Police: Politie Suite Handhaving-Vreemdelingen (PSHV) Marechaussee: Vreemdelingen Basissysteem (VBS), Sigma IND: Indigo

					Generic: Basis Voorziening Vreemdelingen (BVV)
- *birth name*	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	In databases	Police: PSHV, BVV Marechaussee: VBS IND: Indigo Generic: BVV
- *previous name(s)*	1, 2, 3	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1, 2, 3) - Central Agency for the Reception of Asylum Seekers (COA) (1, 2, 3)	- oral (interview face-to-face)	In databases	Police: PSHV Marechaussee: VBS IND: Indigo COA: Integraal Bewoners Informatie Systeem (IBIS)
- *pen name (alias)*	2	-National Police or Royal Netherlands Marechaussee	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS
- *religious names*					
- *other names*					

Sex	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	In databases	Police: PSHV, BVV Marechaussee: VBS Generic: BVV
Biometric data					
- *photo*	1	-National Police or Royal Netherlands Marechaussee	- identification unit	In databases	Police: PSHV, BVV Marechaussee: VBS Generic: BVV
- *fingerprints (which fingers, rolled or pressed fingerprints)*	1 10 fingers, rolled and pressed	-National Police or Royal Netherlands Marechaussee (1, 2)	- identification unit	In databases	Police: BVV Marechaussee: VBS Generic: BVV
- *iris scan*					
- *other*					
Eye colour					
Height					
Date of birth	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	In databases	Police: PSHV Marechaussee: VBS IND: Indigo Generic: BVV
Citizenship(s)	1, 1.1	-National Police or	- analysing documents (as far as	In databases	Police: PSHV

		Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1)	available) - oral (interview face-to-face) - written questionnaire - online self-registration		Marechaussee: VBS IND: Indigo Generic: BVV
Country of origin	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1) - Central Agency for the Reception of Asylum Seekers (COA) (1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	In databases	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS Generic: BVV
Place of birth					
- *town*	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and Naturalisation Service (1.1)	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire - online self-registration	In databases	Police: PSHV Marechaussee: VBS IND: Indigo Generic: BVV
- *region*	1.1	- Immigation and Naturalisation Service	- oral (interview face-to-face) - online self-registration	Electronic file	Indigo
- *country*	1, 1.1	-National Police or Royal Netherlands Marechaussee (1) - Immigation and	- analysing documents (as far as available) - oral (interview face-to-face) - written questionnaire	In databases	Police: PSHV Marechaussee: VBS IND: Indigo

		Naturalisation Service (1.1)	- online self-registration		Generic: BVV
- *other*					
Date of arrival in the (Member) State	1, 1.1, 2	-National Police or Royal Netherlands Marechaussee (1, 2) -Immigration and Naturalisation service (1.1)	- oral (interview face-to-face) - online self-registration - written questionnaire - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo
Last place of residence in the country of origin	1, 1.1, 2	-National Police or Royal Netherlands Marechaussee (1, 2) -Immigration and Naturalisation service	- oral (interview face-to-face) - online self-registration - written questionnaire - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo
Last place of residence before entry in the (Member) State	1, 1.1, 2	-National Police or Royal Netherlands Marechaussee (1, 2) -Immigration and Naturalisation service (1.1)	- oral (interview face-to-face) - online self-registration - written questionnaire - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo
Contact details					
- *phone number*	2	-National Police or Royal Netherlands Marechaussee -Central Agency for the Reception of Asylum Seekers (COA)	- oral (interview face-to-face)	Electronic file	Police: PSHV Marechaussee: VBS COA: IBIS

- *email address*	2	-National Police or Royal Netherlands Marechaussee -Central Agency for the Reception of Asylum Seekers (COA)	- oral (interview face-to-face)	Electronic file	Police: PSHV Marechaussee: VBS COA: IBIS
- *current address*					
- *other*					
Civil status	2 , 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service -Central Agency for the Reception of Asylum Seekers (COA)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS
Accompanied by:					
- *spouse or civil partner*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3) -Central Agency for the Reception of Asylum Seekers (COA) (1, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS

- *children*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3) -Central Agency for the Reception of Asylum Seekers (COA) (1, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS
- *parents*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service -Central Agency for the Reception of Asylum Seekers (COA) (1, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS
- *other relatives*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3) -Central Agency for the Reception of Asylum Seekers	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS

		(COA) (1, 3)			
Family members in the (Member) State					
- *name*	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
- *residency*	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
- *citizenship*	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
- *other*					
Family members in another (Member) State	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Close relatives in the (Member) State	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Close relatives in another (Member) State	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Health status					**Health s**
- *specifics on health status*	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
- *reference that a general health check has been carried out*	3	Immigration and Naturalisation service	Letter from the organisation which executes the health checks	Electronic file	Indigo

- *other*					
Education					
- *school attendance*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3) -Central Agency for the Reception of Asylum Seekers (COA) (3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS, Personal Logbook
- *academic studies*	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV Marechaussee: VBS IND: Indigo COA: IBIS, Personal Logbook
- *trainings*	3	-Central Agency for the Reception of Asylum Seekers (COA) (3)		Electronic file	COA: IBIS, Personal Logbook
- *apprenticeships*					
- *non-formal work experience*					
- *other*					
Language skills	3	-Central Agency for the Reception of			COA: IBIS, Personal Logbook

		Asylum Seekers (COA) (3)			
Profession	1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (2) -Immigration and Naturalisation service (1.1, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Indigo
Criminal record	1, 3	National Police (1) - Immigration and Naturalisation service (3)	using automated or artificial intelligence for analysis of data - oral (interview face-to-face) - online self-registration	Electronic file	PSHV Indigo
Financial resources	1, 2 (cash available)	-National Police or Royal Netherlands Marechaussee (1, 2)	lugage check	Electronic file	Police: PSHV KMar: VBS
Supporting documents					
- passport	1	-National Police or Royal Netherlands Marechaussee	- analysing documents (as far as available) - oral (interview face-to-face)	In databases	Police: PSHV, BVV Marechaussee: VBS Generic: BVV
- travel document	1	-National Police or Royal Netherlands Marechaussee	- analysing documents (as far as available) - oral (interview face-to-face)	In databases	Police: PSHV, BVV Marechaussee:

					VBS Generic: BVV
- other	1, 3	-National Police or Royal Netherlands Marechaussee (1) -Immigration and Naturalisation service (3)	- analysing documents (as far as available) - oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
Reasons for fleeing	1, 2, 3	-National Police or Royal Netherlands Marechaussee (1)[55] -Immigration and Naturalisation service (2, 3)	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
Reasons for not wanting to be returned to the competent Member State as part of a Dublin procedure	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Previous applications	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Information on the route taken	1, 1.1, 2, 3	-National Police or Royal Netherlands Marechaussee (1) -Immigration and Naturalisation service (1.1, 2, 3)	- oral (interview face-to-face) - online self-registration	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
Information on exclusion	3	-Immigration and	- oral (interview face-to-face)	Electronic file	Indigo

[55] If necessary for proper identification in the identification and registration process it is possible to ask for the reasons for fleeing, but in most cases this question is not asked until the examination phase

grounds		Naturalisation service			
Religious affiliation	3	-Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Indigo
Vulnerabilities					
- *Unaccompanied minor*	1, 2, 3	-National Police or Royal Netherlands Marechaussee (1, 2, 3) -Immigration and Naturalisation service (1, 2, 3) -Central Agency for the Reception of Asylum Seekers (COA) (3)	- oral (interview face-to-face) -analysing documents (when available) -age check	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo COA: IBIS
- *Pregnant*	1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
- *Disabilities (which?)*	1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
- *Elderly*	1, 2, 3	-National Police or Royal Netherlands Marechaussee	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV

		-Immigration and Naturalisation service			Marechaussee: VBS IND: Indigo
- *Single parent with minor child(ren)*	1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
- *Victims of human trafficking*	1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service -Central Agency for the Reception of Asylum Seekers (COA) (3)	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo COA: IBIS
- *Mental disorders*	1, 2, 3	-National Police or Royal Netherlands Marechaussee -Immigration and Naturalisation service	- oral (interview face-to-face)	Electronic file	Police: PSHV, BVV Marechaussee: VBS IND: Indigo
- *Victims of torture, physical or sexual violence (female genital mutilation)*	3	-Immigration and Naturalisation service	- oral (interview face-to-face) - online self-registration	In database (not in structured form)	Indigo
- *other*					

Other (please specify)					

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)

No, only information collected by authorities who are directly connected to the asylum procedure is used in the asylum procedure. This information is loaded immediately in the BVV.

The Netherlands has identified good practices in frontloading information by the authorities connected to the asylum procedure. Please see below.

To secure a uniform use of personal data by all authorities connected to the asylum procedure, these authorities use BVV. Once a foreign national is identified and registered, all connected authorities make use of these data, which will be frontloaded. Adding to or adapting from these data is regulated very strictly.[56]

Once a foreign national is registered in the BRP by the municipality, these personal data will be frontloaded in BVV and in this way to all connected systems. In this way a foreign national is known to all the relevant authorities with the same personal data. More information about BVV and BRP: Box 3

Asylum seekers are first registered in the BVV and at the end of the registration procedure the connection with the BRP is made. While other foreign nationals might be registered first in the BRP and this information is frontloaded automatically into the BVV.

This is considered a good practice for all connected authorities, because it avoids confusion through differences in personal data for one person. This is mentioned as a good practice in interviews with the Police, the Royal Netherlands Marechaussee, the Dutch Council for Refugees.[57]

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 4

Database	Overview/definition of the database (please indicate whether it is a regional, national or European database).[58]	National authorities that have access to the databases or access to its data[59]			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	For what purpose	Type of data	For what purpose

[56] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.
[57] Interview with experts from National Police on 23 April 2020, Royal Netherlands Marechaussee on 21 April 2020 and Ministry of Justice and Security on 28 April 2020.
[58] All databases stated under 'primary' and 'secondary' databases are national. There are no regional databases. The European databases used into the asylum process are stated in a different table.
[59] 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.

			procedure			
Primary national databases used in the Netherlands for the purpose of data management in the asylum procedure[60]						
Smartflow	Smartflow is a system in which data is registered by the IND. Applicants for international protection are registered in this system on the basis of a so-called "*smartflow number*".[61]	Access to database: - IND - Police - COA	Registering an application Lodging an application	Applicants for international protection are registered in this system on the basis of a so-called "*smartflow number*".[62] The smart flow number helps to track the asylum seeker in the systems until a so-called V-number[63] has been assigned.	None	None
Basisvoorziening Vreemdelingen (BVV)	Central shared database with basic information on applicants	Access to database: - DT&V - KMAR - IND - Police - COA - DJI - the Ministry of Foreign Affairs - Seaport Police - the Council for Legal Aid (RvR) - The Citizen Service Number Management (BV	Throughout the entire asylum procedure	The BVV is the central information system of organisations that cooperate in the migration process[64] in which all basic data of third-country nationals in the Netherlands has been recorded. [65]	Biometric data; Personal data;[66] Legal information;[67] Address.[68]	Check in VIS and Eurodac

[60] EMN The Netherlands has distinguished between 'primary systems' and 'secondary systems' to clarify between the systems used in the process itself (primary systems) and other, more specific systems used by the organizations itself (secondary systems). The databases in the Netherlands are all interconnected (through the BVV).
[61] Security and Justice Inspectorate (2016). Vervolgonderzoek de identificatie van asielzoekers in Nederland (''Follow-up research into the identification of asylum seekers in the Netherlands) (in Dutch), p. 28.
[62] Security and Justice Inspectorate (2016). Vervolgonderzoek de identificatie van asielzoekers in Nederland (''Follow-up research into the identification of asylum seekers in the Netherlands) (in Dutch), p. 28.
[63] The V-number is an unique number that identifies every third country national at the IND and the organization cooperating in the immigration processes (such as the Immigration Police (AVIM)). This number is assigned as soon as someone starts an application procedure. The number is stated in all correspondence that the third country national or sponsor receives from, among others, the IND. It is also stated on the residence document itself. Moreover, it's also worth mentioning that other immigrants (e.g. EU-citizens) may get a V-number.
[64] Immigration and Naturalisation Service (IND), Custodial Institutions Agency (DJI), Repatriation and Departure Service (DT&V), National Police, Royal Netherlands Marechaussee, Ministry of Security and Justice, and Ministry of Foreign Affairs.
[65] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.
[66] Including: first name, last name, nationality, picture.
[67] Including: permit, status, titles, procedures
[68] COA submits the address of the location where the asylum seeker lives.

		BSN) through the National Office for identity Data (RvIG). Access to data: - The Inspectorate of Social Affairs and Employment - municipalities - Judicial Information Service (JustID).				
Municipal Personal Records Database (Basisregistratie Personen, BRP)	The BRP is the personal records database for all residents of the Netherlands. This includes nationals as well as third-country nationals residing legally in the Netherlands (for a longer period).	Municipalities (access to database) Access to data can be provided to: government institutions who need the data for the execution of their tasks (e.g. the National Tax Authority); organisations with important social tasks (e.g. pension funds, hospitals and insurers); Research institutions for the purpose of scientific, statistic or historic research. Incidental access to the data can also be provided, e.g. to citizens, municipal services or organisations with judicial tasks.[69]	Examination of the application	All residents in the Netherlands must be registered in the BRP. For asylum seekers, registration is done in any case as soon as the applicant receives the asylum status or after 6 months in procedure for asylum. In addition, there is a new possibility to register as soon as the identity of the applicant is sufficiently established and the expectation is that the applicant will stay at least 4 months in the Netherlands. Through registration in the BRP, asylum seekers can more quickly receive	None	None

[69] For more information please see: National Office for Identity Data, 'Users of the BRP,' https://www.rvig.nl/brp/gebruikers-van-de-basisregistratie-personen-brp, consulted on 19 October 2020.

				a citizen service number (BSN), so that they can arrange a bank account and government services sooner.		
Secondary national databases used in the Netherlands for the purpose of data management in the asylum procedure						
INDiGO	INDiGO is the IND's client information system. In INDiGO, both biographical and biometric data are registered. INDiGO is linked to the BVV.	IND (access to database)	Throughout the entire asylum procedure	All cases in which the IND plays a role are handled in INDiGO.	Biometric data (fingerprints) and personal data	Requests for taking charge and requests for taking back on the basis of Regulation (EU) No 604/2013. This data is shared through the standard form of the European Commission.
Integral Residents Information System (Integraal Bewoners Informatie Systeem, IBIS)	Integral Residents Information System (IBIS) is COA's primary system.	COA (access to database)	Lodging an application	To enable COA to develop, determine and implement an adequate reception policy, COA registers asylum seekers' data in the IBIS.	Personal, guidance methodology, financial, logistic, legal information	To support COA to register all residents' information; to determine whether there is still a right to receptio

						n.
Police Immigration Enforcement Suite (Politiesuite Handhaving Vreemdelingen, PSHV)	The PSHV registers both biometric and biographical data which are copied to the BVV. The PSHV is linked to the Central Shared Database With Basic Information On Applicants (BVV).	National Police (access to database)	Making an application, lodging an application	In the PSHV all personal data is recorded of third-country nationals who come into contact with the National Police. The PSHV contains all aspects of immigration law and is used by the Immigration Police Identification and Human Trafficking Department (AVIM). It provides an overview of all files.[70]	None	None
Immigrants Basic System (Vreemdelingen Basissysteem, VBS)	The VBS contains data on third-country nationals with whom the KMar and Seaport Police have been in contact. Sections of the VBS are copied to the BVV.	- KMar (access to database) - Seaport Police (access to database)	Making an application, lodging an application	The VBS is used by the KMar and the Rotterdam Seaport Police for the registration of biometric and biographical data. It is linked to the BVV and used in all KMar's processes involving third-country nationals, such as asylum.	N/A	N/A
Additional information As seen in Q12 several European databases are used (e.g. Eurodac). For the purpose of the answer to this question and this table, no European databases are mentioned since these are already mentioned under the question on 'cross-checking' (e.g. Q24).						

Box 3: the main tools used in data management in the asylum process

[70] Security and Justice Inspectorate Report De Identificatie van asielzoekers in Nederland ("The Identification of asylum seekers in the Netherlands") (November 2016), p.19 (in Dutch).

1. Basic Facility for Identity Establishment (Basisvoorziening Identificatie, BVID).

The Basic Facility for Identity Establishment (*Basisvoorziening Identificatie, BVID*) is the main tool in the identification and registration process of third-country nationals, including asylum seekers. BVID is not a database but a facility used by the Police and KMar to consult and enter data in connected databases, including the Central Shared Database with Basic Information on Applicants (see below). The so-called "BVID Kiosk" contains a document scanner, fingerprint scanner and photo camera that are connected to a computer. At the BVID Kiosk the asylum seeker's fingerprints are taken digitally and a face picture is taken. Any available travel and/or identity documents are also read in the BVID Kiosk.[71]

2. Central Shared Database With Basic Information On Applicants (*Basisvoorziening Vreemdelingen, BVV*)

The Central Shared Database With Basic Information On Applicants (*Basisvoorziening Vreemdelingen, BVV*) is the central information system used by organisations cooperating in the immigration process in which all basic data of third-country nationals and EU-citizens in the Netherlands is recorded. This concerns personal data, card data, document data as well as procedural data. The BVV is used exclusively in the following migration procedures for the registration and modification of data: asylum, repatriation, visa, and legal migration (remunerated activities, study, family). Additionally, it is also used for supervision purposes (including registration of third-country nationals found to be staying illegally and not formerly known to the organisations involved).

Data exchange

The BVV has no direct users. The cooperating partners use their own process support systems that are connected to the BVV via XML message traffic, or ebXML message traffic.[72]

3. V-number

Upon first registration of the third-country national in the BVV, a unique number, the V-number, is assigned. The V-number is a unique number that identifies every third country national at the IND and the organization cooperating in the immigration processes (such as the Immigration Police (AVIM)). This number is assigned as soon as someone starts an application procedure. The number is stated in all correspondence that the third country national or sponsor receives from, among others, the IND. It is also stated on the residence document itself. Moreover, it is also worth mentioning that other immigrants (e.g. EU-citizens) may get a V-number.[73]

4. Municipal Personal Records Database (BRP)

Besides the BVV the Netherlands has its Municipal Personal Records Database (BRP). In the BRP, biographic data is registered. The BRP is used in the asylum procedure. The asylum seeker is registered when he/she has been in the asylum procedure and has the opportunity to stay for a longer period.

The BRP is the personal records database for all residents of the Netherlands, including third-country nationals residing in the Netherlands (for a longer period). Persons must be registered in the BRP if they are expected to reside in the Netherlands for a period longer than three months. They must request registration in the BRP through the municipality in which they reside.

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?

[71] Inspectorate of Security and Justice (IVenJ) (2016). *De identificatie van asielzoekers in Nederland* of April 2016 (in Dutch).
[72] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 43.
[73] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.

If an asylum applicant asks for asylum at an authority who is not appointed by the Ministry of Justice and Security[74], the applicant will be redirected to the nearest police station or brigade location of the Royal Netherlands Marechaussee. Basic information on where to go to receive transportation and to register an asylum application is provided.

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

As stipulated under section 1, the registration and lodging phase are for many asylum seekers carried out at the same time in the Netherlands. EMN The Netherlands has decided to skip this section. Please go to section 3.3.

12. Against which databases at i. local/regional, ii. national, iii. European and iv. international levels is the information collected during registration cross-checked[75] (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)

[74] Vreemdelingenbesluit 2000, Artikel 3.108 (Immigration Decree) states that an application for a resident permit must be lodged at a location appointed by the Minister of Justice and Security. Therefor all asylum seekers will be redirected to a location where registration can take place and onward to the location where they can officially lodge their application.
[75] 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).

3.2 Information provided to asylum applicants in the registration phase

As stipulated under section 1, the registration and lodging phase are for many asylum seekers carried out at the same time in the Netherlands. EMN The Netherlands has decided to skip this section. Please go to section 3.3.

15. Are asylum applicants provided with a processing/privacy notice[76] about the personal data collected from them during the registration phase?

    ☐ 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?

[76] 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.

Yes, the Netherlands provides for a partial self-registration procedure for asylum seekers (during the **registration/lodging** phase of the asylum procedure – please see also box 2). It has been developed and introduced in 2015 and 2016. The digital registration form (or customer form) serves to retrieve as much information from the asylum seeker as possible before the asylum process starts. The aim of the digital application form is efficiency, by digitizing the once written customer form. By (a) letting the customer fill in the digital form himself; (b) automatically translate data[77]; (c) to reuse this data, the registration process is facilitated.

20. Where do asylum seekers self-register (e.g. website, by phone)?

Through a special program on a computer provided by the IND that generates the digital application form.

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

Yes, an employee from the IND opens the digital application form, installs the correct language and helps/guides the asylum seeker (in person) if he/she has any questions. When the asylum seeker is finished with the digital application form the employee assists the asylum seeker to another location/room.

22. In which languages is the self-registration procedure available?

At the moment the digital application form is available in the following languages:

- Albanian
- Amharic
- Arabic (general)
- Bosnian
- Croatian
- Dari
- English
- Farsi
- French
- Pashtun
- Punjabi
- Russian
- Serbian
- Spanish
- Tigrinya
- Turkish
- Urdu

23. Is self-registration mandatory or optional?

Please elaborate.

The digital self- registration is optional. It can also be done in writing.

[77] Automatic translation is partial implemented. The rest is translated by registered interpreters.

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)?

Information is cross-checked against national, European and international databases. Please see below.

In general

There are several ways through which data of asylum seekers are checked against other databases.

- The BVID Kiosk is the main tool in the identification and registration process of third-country nationals, including asylum seekers. The BVID Kiosk contains a document scanner, fingerprint scanner and photo camera that are connected to a computer. Various (biometric) characteristics of the asylum seeker are entered in the BVID Kiosk, and connected databases (including BVV, Havank, EU-VIS and Eurodac) are consulted. If the asylum seeker is detected in any of these databases, an automatic notification is given. Furthermore, at the BVID Kiosk the asylum seeker's fingerprints are taken digitally and a face picture is taken. Any available travel and/or identity documents are also read in the BVID Kiosk.78 This is done during the phase of making an application and the lodging phase.

Local/regional databases

There is no cross-checking of data against local/regional databases because there are no local/regional databases.

National databases

- BVV (Central shared database with basic information on applicants): the purpose is to check, when registering, whether the data already exists, to avoid double registrations. Through the BVV also other databases are automatically searched, e.g.
- HAVANK: the automated fingerprint recognition system of the National Police. Its purpose is to search for information available on finger prints.

European databases

- Eurodac: the purpose is to search for information available on finger prints and to check if there are any other (Member) States that are responsible for the asylum seekers application.79
- European system for short-stay visas (EUVIS): the purpose is to search for information available in this system in regards to short-stay visas.
- Schengen Information System (SIS II): the purpose is to search for any additional information of the asylum seeker, also in regards to any earlier registrations somewhere else within Schengen.

International databases

- Stolen and Lost Travel Documents Database: the purpose is to see whether any documents that the asylum seeker puts forward are in this database.

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

☒ Yes / ☐ No

Yes. Via the BVID Kiosks and during the examination of all data received during the identification of the asylum seeker, the underlying systems, including VIS and SIS, are searched for all asylum seekers. [80]

[78] Inspectorate of Security and Justice (IVenJ) (2016). *De identificatie van asielzoekers in Nederland* of April 2016 (in Dutch).
[79] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.
[80] Interview with experts from the Ministry of Justice and Security on 28 April 2020.

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)

There are issues that are encountered in cross checking data collected at the registration/lodging phase. No issues were found in (national) reports. The issues mentioned below were mentioned by experts which were interviewed for the purpose of this study (please see box 1).

- An expert of the IND notes that if there is a technical issue with the databases of partner organisations, cross-checking cannot be carried out. Being dependent on other organisations and the need to contact partner organisations prior to accessing data are considered as challenges.[81]
- Experts from the Ministry of Justice and Security note that since information has been recorded in the BVV (and its predecessor) for a long time, in individual cases information from relatively long ago may emerge upon registration. In such cases additional investigation is needed to understand where this data comes from, leading to an increased workload.[82]
- Lastly, experts from the Police mention that cross-checking may return a large amount of information since multiple databases (including VIS, SIS, Eurodac) are queried, each based on a large amount of documents and information. If a deviation in information is noticed during this cross-check, the system gives a notification. In cases where there is real doubt about the identity of the applicant, such deviations need to be further investigated, e.g. by reading data carriers. This leads to an additional workload, even though the data concerned may sometimes be relatively outdated.[83]

4.2 Information provided to asylum applicants at the lodging phase

28. Are asylum applicants provided with a processing/privacy notice[84] about the personal data collected from them during the lodging phase?

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).

Yes, at the beginning of the **registration** phase every asylum applicant receives a brochure explaining the asylum procedure in the Netherlands. There are different brochures for different steps or channels in the asylum procedure. The brochures explain the different steps of the registration process, the organisations involved, the "rest and preparation time" and the processing of the personal data.

All brochures are available in different languages and can be further explained with an interpreter by a volunteer of the Dutch Council for Refugees during the "rest and preparation time[85]".

The brochures are handed out either by the police (AVIM), the Royal Netherlands Marechaussee or the Immigration and Naturalisation Service, during the registration process there are checks to make sure the

[81] Interview with an expert from the IND on 30 April 2020.
[82] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[83] Interview with experts from the Police on 23 April 2020.
[84] 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.
[85] Interview with experts from the Dutch Council for Refugees, on 14 May 2020.

necessary information is provided and explained.

In all brochures handed out in the asylum procedure the following information is provided:

Personal data is all kinds of information about you. The organisations that have cooperated in this leaflet are listed below. These organisations handle personal data during the processing of your application, notification or request. They ask you for your details and also ask other organisations or people for these, if necessary. These organisations use and store your details and pass them on to other organisations if that is required by law. The privacy legislation contains obligations for organisations that process your data. For example, they must handle your data safely and with due care.
The privacy laws also set out your rights, for example:
• to consult the data held by organisations;
• to know what the organisations do with your data and why;
• to know to which organisations your data has been passed on.
Do you want to know more about the processing of your personal data and your rights? Check the websites of the organisations.[86]

Furthermore, in the Privacy Statement all clients of the IND, including asylum applicants, can find information about the data that is collected and for what purpose this is collected.[87]

As part of the **registration** phase the applicant will furthermore sign his application (form M35-H), this is done under the supervision of the police or the Royal Netherlands Marechaussee. This form contains the processing/privacy notice and the information is explained to the applicant. With the signing of this form the application is officially **lodged** and the applicant gives permission for the use and collection of his personal information during all phases of the asylum procedure.[88]

In the registration interview (*aanmeldgehoor*) the asylum applicant is specifically explained that none of the provided information in relation to the asylum procedure will be given to officials of the country of origin.[89]

And during the registration interview the applicant is asked to sign a consent statement in which permission is given to share limited special personal data with the municipalities on which is based the registration in the BRP. This is a temporary procedure installed in 2017, which is effective until new legislation to fully formalize this exchange of information will enter into force. This request is accompanied by an explanation in a wide range of languages of the intended use of the given information.[90]

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

The brochures are joint productions of the Central Agency for the Reception of Asylum Seekers, the Repatriation and Departure Service, the Immigration and Naturalisation Service, the Legal Aid Board and the Dutch Council for Refugees. The brochures are commissioned by the Directorate for Migration Policy of the Ministry of Justice and Security.

Most of the brochures will be handed out during the registration phase, but as the need arises they can also be provided to the applicant during the examination phase. This might be the case if the applicant is changed to a different procedural channel. After the application for asylum is signed, the application is lodged and an employee of the Immigration and Naturalisation Service will hold a registration interview with the applicant. In this interview the applicant will be asked if he has received the brochure(s) that apply

[86] Dutch Council for Refugees, 'Before your asylum procedure begins,' https://www.vluchtelingenwerk.nl/sites/default/files/u32918/rvt_2020_-_en_-_digi.pdf, accessed 23 November 2020.
[87] Immigration and Naturalisation Service, IND Privacy Statement, https://ind.nl/en/documents/privacy_statement_ind.pdf, accessed 20 November 2020.
[88] Section A6/ Model M35-H of the Immigration Act Implementatin Guidelines (Vc) 2000: https://wetten.overheid.nl/BWBR0012287/2020-07-09#BijlageM35.H
[89] This information was provided by the IND on 2 June 2020
[90] Immigration and Naturalisation Service, written information provided on 26 November 2020

to his procedure and if he has read them and understands them. If necessary brochures will be supplied and time and explanation will be given during the registration interview to make sure the applicant is fully aware of the information provided.

The interviewer will explain that all information provided by the applicant during his procedure will be treated as confidential information. The information will not be shared with other parties without his consent unless this is necessary under Dutch laws[91].

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

Please describe.

All three:

- There are brochures available in different languages.
- The procedure and reason for data collection is explained orally at different stages in the procedure.
- On the websites of the different organisations operational in the immigration process, the privacy statement of that organisation is published. This statement is available in Dutch and English92.
- On the website www.ind.nl information about the asylum procedure is available in Dutch and English. Also the afore mentioned brochures can be downloaded here in the available languages.

The Dutch Council for Refugees has a special website for refugees with information about the asylum procedure and a link to the brochures (https://www.vluchtelingenwerk.nl/forrefugees/asielprocedure)[93]

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)?

Yes, interpretation is available. According to Dutch law the applicant has the right to the use of an interpreter during his asylum procedure if this is necessary to provide good communication94.

The interpreters are independent and are commissioned per case to interpret the interview between the Immigration and Naturalisation Service and the asylum applicant.

The interpreters are also commissioned by the Dutch Council for Refugees and the lawyer when the asylum applicant is prepared for the interviews or when the account of the interview is reviewed.

Interpreters can be available in person or via telephone.

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

☒ Yes / ☐ No

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

Yes, translation is at least available in English.

All organisations involved in the asylum procedure have websites available in Dutch and English. These are both national authorities and NGOs.

The website of the Dutch Council for Refugees (NGO) is available in Dutch, Farsi, Arabic, English, Dari,

[91] Standard interview format Immigration and Naturalisation Service

[92] For more information see: Immigration and Naturalisation Service, 'IND Privacy Statement,' https://ind.nl/en/documents/privacy_statement_ind.pdf; www.coa.nl; www.politie.nl

[93] This information was provided by the Council for Refugees on 26 May 2020

[94] Section 3.109a, sub 1, Immigration Decree (Vb)2000

Tigrinya, French and Somali[95].

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)?

Yes, the brochures with information about the asylum procedure are available in the languages: Arabic, Armenian, Chinese, Dari, English, Farsi, French, Mongolian, Russian, Serbo-Croatian, Somali, Tigrinya and Urdu. Some of the other brochures are also available in Albanian, Hindi, Macedonian, Ukrainian, Azeri, Sorani, Tamil, Turkish and Amharic. It depends on who will benefit the most of the brochure in which languages the brochure is translated. (See answer to question 16 a for the organisations involved).

Explanation of the written information, if it is not available in a language that applicant can read, is given either by a volunteer of the Dutch Council for Refugees or the assigned legal aid with the help of an interpreter.[96]

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

Yes, all staff in the registration process is trained in the use of the registration systems. As guideline for the correct registration there is a protocol written which is available for al personnel. This is the Protocol Identification and Labelling (PIL).

For staff of the IND an online training is available to learn about the Privacy Laws (GDPR/AVG) and the impact in the registration phase. [97]

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)?

The examination starts when the rest period (*rust en voorbereidingstijd*) has ended. Then, the IND moves on to examining the application of the asylum seeker. During the examination phase, information is **not** cross-checked against local/regional, national, European and international databases. All information is already checked in databases by the National Police (AVIM), the Royal Netherlands Marechaussee and the IND before moving on to this phase. The IND does not have access to the systems used by the AVIM, except for VIS and Eurodac. The latter can be accessed by the IND's "Dublin Unit", which can decide to do so in case of doubts about whether the asylum seeker has travelled on a visa.[98]

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

[95] This information was provided by the Council of Refugees on 26 May 2020
[96] Interview with experts from the Dutch Council for Refugees on 14 May 2020.
[97] Information extracted from: Ontwikkelportaal IND / Education site IND
[98] Interview with an expert from the IND on 30 April 2020.

☐ Yes / ☒ No

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).

No challenges to be reported.

5.2 Information provided to asylum applicants at the examination phase

34. Are asylum applicants provided with a processing/privacy note[99] 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)?

Yes, at the beginning of the asylum procedure the applicants are informed about the personal data collected during the whole asylum procedure (application form M35-H and the brochures). The Netherlands does not differentiate in phases in the asylum procedure in accordance to the information provision, so the information provided in the registration phase is intended for the whole asylum procedure. For more explanation, please see the answer to question 28.

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

Please describe.

As stated above in the answers to question 29b information about the use and collection of personal data collected during all phases of the asylum procedure is provided digital on the websites of the organisations involved. This is also the location where the privacy statement can be found. Orally in the meetings with the volunteers of the Council for Refugees, their legal aid or during the interviews with the Immigration and Naturalisation Service. And in writing in the provided brochures that explain the asylum procedure in the Netherlands and in the written transcripts of the interviews. The brochures are translated in different languages, while the transcripts are reviewed with their legal aid/lawyer together with an interpreter.

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)?

[99] 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.

Yes, interpreters are used, either in person or by telephone. The interpreters are independent and are paid for by the Government to assure that the applicant can communicate during his asylum procedure with the necessary organisations[100]

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

☒ Yes / ☐ No

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

Yes, but only in English. All organisations involved in the asylum procedure have websites available in Dutch and English. These are both national authorities and NGOs. Except for the Council for Refugees, their website is available in more languages (see question 29d).

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

X Yes / ☐ No

Yes, all brochures are translated in different languages (see question 29e for languages).

All other documents are explained by either the designated lawyer or a volunteer of the Council for Refugees together with an interpreter.

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

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

Staff of the Immigration and Naturalisation Service is trained in registering data necessary for the asylum procedure and in the use of the database (INDIGO) in which the registration and examination of the asylum application takes place.[101]

Also an online training is available to learn about the Privacy Laws (GDPR/AVG)[102]

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

If yes, please elaborate on some contrasting[103] examples of data quality assessment and indicate:

Yes, the quality of the data (alphanumeric and biometric) collected during the asylum procedure is assessed (e.g. with regard to accuracy, timeliness, completeness, consistency, duplication and validity of the data).

[100] Section *3.109a, sub 1, Immigration Decree (Vb)2000*

[101] Information extracted from *INDIGO opleidingen / Education site IND*

[102] Information extracted from *Ontwikkelportaal IND / Education site IND*

[103] 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.

Data quality assessment in databases:

- The BVID Kiosk is the main tool in the identification and registration process of third-country nationals, including asylum seekers. The BVID Kiosk contains a document scanner, fingerprint scanner and photo camera that are connected to a computer. Various (biometric) characteristics of the asylum seeker are entered in the BVID Kiosk, and connected databases (including BVV, Havank, EU-VIS and Eurodac) are consulted. The user of the BVID Kiosk is automatically notified if the asylum seeker is detected in any of these databases. Furthermore, at the BVID Kiosk the asylum seeker's fingerprints are taken digitally and a face picture is taken. Any available travel and/or identity documents are also read in the BVID Kiosk.[104] This is done during the phase of making an application and the lodging phase.
- Data is entered in fixed fields, some of which are mandatory to fill in, and there is a possibility to attach documents. The system can create a notification to see if everything is complete.[105] When the name is unknown, the database creates a 'workaround' with a NN-number, with information on the region of origin, sex, date and time of registration.[106]
- Through biometric registration in the BVV the data is connected to the V-number which is used for communication within the asylum process.107 When registering an asylum seeker into the BVV, the database is already checked, in order to avoid double registrations. If the asylum seeker is not found in the system, the BVV issues the unique V-number upon registration.[108] This is done during the phase of registering an application and the lodging phase by the National Police (AVIM) or the KMar.
- Verification takes place by comparing the V-number and one or two fingerprints with the fingerprints of the person concerned that are stored in the BVV. If the asylum seeker has a document containing fingerprints, verification against this document can take place. In case this verification against the document is unsuccessful, a comparison with the fingerprints in the BVV will take place. The identity of an asylum seeker is checked in particular when a relationship is established between the person concerned and a (physically present) foreign national and changes are being made to the asylum seeker's file.[109]
- If search on fingerprints is unsuccessful or not possible, asylum seekers can be searched via an 'intelligent search tool' in the BVV in two ways: using exact search criteria or through a combination of data. Several unique numbers can be used (e.g.) various numbers related to the asylum seeker, but it is also possible to search for combinations of, for example, name details, date of birth, country of birth, etc. With the help of 'intelligent search tool', parts of name data or dates of birth can be searched, for example.[110] This is done throughout the asylum procedure and this tool is available to all organisations which have access to the database.

Data quality assessment by staff:

- During the examination phase the IND carries out a language assessment using the language indicator developed by TOELT.[111.] A language indicator is a short recording (5 - 10 minutes) of asylum seekers. A TOELT language expert assesses the language variant in these recordings and is used to (partly) verify the data regarding nationality.[112]
- Every week a selection of asylum procedures is assessed both for data quality and for the quality of the decision making process. The quality assessment is carried out by senior caseworkers of the

[104] Inspectorate of Security and Justice (IVenJ) (2016). *De identificatie van asielzoekers in Nederland* of April 2016 (in Dutch).
[105] Interview with experts from the Royal Netherlands Marechaussee on 21 April 2020.
[106] This refers to the "NN regiocode geslacht jjmmdd hhmm" system, see: Ministry of Justice and Security, Protocol and Labeling, version 10.2, p. 23.
[107] This information was provided by experts from the Ministry of Justice and Security on 29 May 2020.
[108] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.
[109] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 29.
[110] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 25.
[111] Identity and Document Investigation Unit and the Office for Country Information and Language Analysis. TOELT is a part of the IND that, among other things, carries out language indicators.
[112] Management rapport TOELT January – June 2016, p. 12 (in Dutch)

IND within the guidelines set by the IND Strategy and Implementation Advice Department. Quarterly a report is made by this department for the Management Board of the IND. If during the quality assessment omissions in data in individual cases are found, these will be addressed and the original case worker will have to amend these omissions.[113] Moreover, other analysis on data is carried out and discussed at several meetings within the Ministry of Justice and Security.[114]

- In the Netherlands there is also a platform wherein ID-experts (Ketenplatform Identiteit) discuss any issues regarding data. The platform addresses three main topics: quality of the (ID) data used by organisations cooperating in the immigration process, (complex) cases and issues that might go further than immigration (e.g. criminal law).[115]

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

The quality of data is assessed in all phases of the asylum procedure.

b) How (specific tools)[116] and by whom (centralised/decentralised) is the quality assessment carried out?

- Screening for duplicates against data already stored in the database upon registration in the BVID Kiosk is carried out by the KMar and the AVIM unit of the NP. Throughout the asylum procedure in the BVV (carried out by all organisations that have access to the BVV)
- Automated data quality checks upon registration in the BVID Kiosk are carried out by the NP and KMar
- Verifying identity through language assessments and during the interview us carried out by the IND
- Weekly sample checks of asylum procedures are carried out by senior caseworkers of the IND

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

- The central database (BVV) is supported by software that handles data exchange with the organisations cooperating in the immigration process. The data is exchanged using standard XML messages. For the physical handling of these messages, the BVV is equipped with specific software, a so-called message broker. The organizations cooperating in the immigration process also have such a facility. The BVV has no direct users. The cooperating partners use their own process support systems that are connected to the BVV via XML message traffic, or ebXML message traffic.[117]
- Organisations cooperating in the immigration procedure can “subscribe” to files in the BVV so that they are automatically informed if partner organisations carry out actions related to this file.[118]
- If organisations cooperating in the immigration procedure come across personal data that deviate from the data registered in the BVV, they assess which data is of higher quality. If the data in the BVV is maintained, the deviating data is only entered in the organisation’s own database without consequences for the BVV. Otherwise, the amendment procedure is followed to change data in the BVV.119 If the BVV is amended and it is known that the foreigner is registered in other databases, these will be updated accordingly. This is done both manually and automatically, e.g. to update SIS-II an M93-form is prepared for the IND, while the SKDB (criminal law chain database) is updated automatically based on the V-number.[120]

[113] Written input received by experts from the IND on 1 March 2020.
[114] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[115] Please see: https://www.coa.nl/sites/www.coa.nl/files/paginas/media/bestanden/ketenplan_2018-2022.pdf
[116] E.g. name transliteration, screening for duplicates against data already stored in the database, automated data quality checks, data analytics, artificial intelligence.
[117] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 43.
[118] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 44.
[119] For more information, see Protocol Identification and Labelling 10.2, p. 33-34.
[120] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 34.

- The IND is authorized to change data in the BVV (through INDiGO) independently or in some cases through AVIM or KMar. Where the IND changes data independently, AVIM and KMar are notified manually. Furthermore, staff are asked to always indicate the reason for the change in INDiGO.[121] If the asylum seeker is already registered in the Municipal Personal Records Database (BRP), the amendment must be requested in INDiGO to the municipality where the asylum seeker stays or lives. Once the data is changed in the BRP, the BVV and INDiGO are automatically updated.[122]
- When a third-country national's personal data is registered in the BRP, a message will be sent to the IND, and a link with the V-number will be established in the BVV. From the moment the administration number and the Citizen Service Number (BSN) are known in the BVV, changes in the BRP are automatically processed among organisations cooperating in the immigration process. If the BRP data does not correspond to the data by which a person was known by the organisations cooperating in the immigration process, the original data remains accessible as historical data to those organisations that are responsible for identification. As soon as a third-country national leaves the Netherlands and the BRP stops updating the list of personal data, other cooperating organisations can modify again if needed.

38. Do quality assessment measures only apply retroactively? Yes/No.

Yes, but there are also measures (internal IT-checks) in place within some categories of data to ensure the correct data (for example you cannot enter a date of birth before 1910).[123]

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?

Yes, there are preventative measures in place to get the information right at the very beginning. Several examples and safeguards are mentioned below:

- Due to the implementation of the BVID Kiosk information is already registered at the forefront of the process, including biometric data which is difficult to forge.[124] [125] [126]
- Staff working with the BVID Kiosk require a special authorisation to do so. Coordinators from the National Police are tasked with safeguarding the process and supervising personnel. A briefing takes place every morning to let everyone know what to do, thus preventing mistakes.[127]
- The Netherlands created several protocols and instructions (e.g. Protocol Identification and Labeling; ID-checklist from the Police[128] and KMar) to guide the registration process in an optimal way.
- Guidelines and tools are furthermore incorporated into the database (internal IT-checks) to ensure correct data. For example, it is not possible to enter a date of birth before 1910.[129]
- Furthermore, there is an e-learning seminar for all IND case workers and new recruits are given extensive training before starting on the job. [130]

6.2 Safeguards

[121] IND Instruction 2018/12, p. 1-2.
[122] IND Instruction 2018/12
[123] Information provided by experts from the IND on 1 March 2020.
[124] Interview with an expert from the IND on 21 March 2020.
[125] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[126] Interview with experts from the Police on 23 April 2020.
[127] Interview with experts from the Police on 23 April 2020.
[128] Interview with experts from the Police on 23 April 2020.
[129] Written input received by experts from the IND on 27 March 2020.
[130] Written input received by experts from the IND on 27 March 2020.

40. Describe the supervision mechanism for data protection supervision of the personal data collected during the asylum procedure in your Member State.[131]

In general
In the Netherlands, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data. The tasks and powers of the Dutch DPA are described in the General Data Protection Regulation (GDPR), supplemented by the Dutch Implementation Act of the GDPR.[132]

In addition to the AP, personal data is protected by the (national) courts and procedures in the Netherlands. This also contains that decisions made by the Dutch DPA can be tried before a court through the objection and appeal procedures.[133]

Asylum procedure
In the Netherlands, the Dutch Immigration Act regulates the use of personal data and biometrics in detail in addition to the GDPR.[134]

The Dutch Immigration Act also regulates the use of related facilities such as the BVID Kiosk in the immigration process and is recorded in this Act with approval by the data protection official (Functionaris Gegevensbescherming, FG) of the Migration Coordination Department. This data protection official (FG) is independent. On behalf of the Ministry of Justice and Security, the FG supervises the application of and compliance with the GDPR in as far as it concerns the facilities for which they are responsible (such as BVV and SIGMA).[135], [136] The organisations that fall under the Ministry of Security and Justice all have in addition to the supervising FG their own Privacy Officer that is specialized in the GDPR and/or Data Protection Act related to their own organisation.[137]

Additionally, the Dutch Data Protection Authority (AP) advises on new legislative proposals which may affect the asylum procedure in the Netherlands. The AP has done this in the past, e.g. on the use of biometrics.[138]

Additional information[139]
As stated above, within other organisations cooperating in the immigration process, privacy officers are now part of the standard operation structure, e.g. within the IND. At the IND a (temporary) GDPR-program was implemented.[140] The program has mainly focused on making the GDPR known within the IND, setting up the processes and the best possible documentation of agreements that are concluded with partners (e.g. on agreements, data exchange). In addition, various Privacy Impact Assessments (DPIAs)[141] are carried out wherein GDPR related issues are checked. All internal systems of the IND have been assessed.

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

X Yes / ☐ No

[131] 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).
[132] For more information, please see: https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa
[133] This information was provided by an expert on privacy from the IND on 2 June 2020.
[134] Dutch Immigration Act, Article 107
[135] For more information, please see: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/privacy (in Dutch)
[136] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[137] This information was provided by an expert on privacy from the IND on 2 June 2020.
[138] For more information, please see: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-gebruik-biometrische-gegevens-de-vreemdelingenketen (in Dutch)
[139] Interview with an expert on privacy from the IND on 28 April 2020.
[140] It be worth mentioning that all organizations cooperating in the immigration process have gone through so projects to make these organisation compliant with the GDPR (source: Interview with experts from the Ministry of Justice and Security on 28 April 2020).
[141] DPIAs are in place to scrutinize entire systems. If major changes take place, for example major changes in authorizations, a DPIA is not always required, but can usually be solved with a risk analysis. The entity then uses the previously performed DPIA as a basis and look at what the changes could lead to. What does not change does not need to be reassessed.

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, systems are assessed. This is both carried out by the Data Protection Authority (please see Q40) and organizations cooperating in the immigration process. Please see below.

Assessments carried out by the Data Protection Authority (AP):
The BRP has been assessed. The old version of the Municipal Personal Records Database (GBA) has been replaced by the new Municipal Personal Records Database (BRP) together with the newly introduced Register of Non-Citizens (RNI) in 2014/2015. At the request of the Minister of the Interior and Kingdom Relations, the Board for the Protection of Personal Data (CBP) (now AP) has advised on the draft decree of the BRP. The CPB advised to amend the draft decision on a number of points. In its earlier advice on the BRP Act, the AP had already pointed to the overly use of general wording of the article in this Act that regulates the processing of the citizen service number (BSN) by non-governmental bodies. Although the article has been adapted, this can still lead to differences in interpretation. The article therefore needed further clarification, which led to those changes.[142]

Assessment carried out by other entities:
All systems used by the organisations cooperating in the immigration process have undergone a Data Protection Implementation Assessment (DPIA) in the context of the implementation of the GDPR.. These DPIAs have been presented and checked by the FG. Moreover, DPIAs have also been carried out on the BVV, SIGMA and Eurodac.[143] There are no publicly available reports on this.

INDiGO was changed slightly after the DPIA. Before the DPIA information of asylum seekers was available to all employees from the IND. This is being changed. With regards to 'high-profile' cases, it is being checked whether the persons working on these cases are the only ones who have access to these cases. [144]

Before SIGMA was introduced, it was standard for an organization to receive all data from the person surveyed. This is no longer possible due to the DPIA. Organizations now have to ask specific questions for specific data, if necessary. It is indicated that no significant changes have been made to the other systems mentioned above due to the DPIA.[145]

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.*

In the Netherlands, the General Data Protection Regulation (GDPR), supplemented by the Dutch Implementation Act of the GDPR, gives the right to asylum seekers to access, rectify or erase their data.

In addition, asylum seekers have access to their file through their legal representative and can request to see (a copy of) their file based on the General Administrative Law Act *(Algemene wet bestuursrecht*). This cannot be equated with a request for access to the processed personal data on the basis of Article 15 of the GDPR. In other words, there is a difference between already being able to access your documentation because of your asylum procedure and making use of the GDPR to obtain insight into what data is being collected by the IND and for what purpose.[146]

Access
There are arrangements making sure that asylum seekers can have access to their data stored in the national systems used for applications for international protection. The organization responsible for the

[142] For more information, please see: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-nadere-uitwerking-basisregistratie-personen (in Dutch)
[143] Interview with an expert on privacy from the IND on 28 April 2020; Interview with experts from the Ministry of Justice and Security on 28 April 2020; Interview with experts from the Police on 23 April 2020; information provided by an expert on privacy from the IND on 20 November 2020.
[144] Interview with an expert on privacy from the IND on 28 April 2020.
[145] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[146] This information was provided by an expert on privacy from the IND on 5 November 2020.

applications for international protection is the IND. In case an asylum seeker wants to access his/her personal data, he/she can submit a form on the website of the IND (www.ind.nl).[147]

At any moment during the asylum procedure, if an asylum seeker wants to access his/her data he/she can contact one of the organisations cooperating in the immigration process at the centre where he/she is staying, if needed with the assistance of his/her provided legal aid.

Rectification
There are arrangements making sure that asylum seekers can rectify their data stored in the national systems used for applications for international protection. The organization responsible for the applications for international protection is the IND. In case an asylum seeker wants to rectify his/her personal data, he/she can submit a form on the website of the IND (www.ind.nl).[148]

If an asylum seeker wants to rectify his/her data during the asylum procedure, he/she can step forward to one of the organisations cooperating in the immigration process at the centre where he/she is staying. There are multiple ways to do so (e.g. during the process of hearing, providing extra documents).[149]

Erasure
There are arrangements making sure that asylum seekers can erase their data stored in the national systems used for applications for international protection. The organization responsible for the applications for international protection is the IND. In case an asylum seeker wants to erase his/her personal data, he/she can write a form on the website of the IND (www.ind.nl).[150] However, some data cannot be legally destroyed by the IND. The IND is bound by the Archive law, to archive certain (basic) information for the goal of demographic figures and historical purposes.151 Furthermore, an asylum seeker has to be mindful that when requesting erasure of certain data, this might have consequences for his or her permit.[152]

Additionally, it may be noted that organizations cooperating in the immigration process are also themselves taking action to erase data. Numerous personal data are registered and processed in the BVV. Pursuant to legislation and regulations, 'cleaning' actions are regularly carried out on these data under the responsibility of the platform for identity experts (*Ketenplatform Identiteit*). This includes the destruction of biometric data after the expiry of a set period.[153]

Available statistics
There are no statistics available on the above mentioned issues.

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

[147] For more information, please see: https://ind.nl/Paginas/Privacy.aspx
[148] For more information, please see: https://ind.nl/Paginas/Privacy.aspx
[149] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.
[150] For more information, please see: https://ind.nl/Paginas/Privacy.aspx
[151] This information was provided by an expert on privacy from the IND on 2 June 2020.
[152] This information was provided by an expert of the IND on privacy on 20 November 2020.
[153] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2.

☐ Legal obstacles

☐ Cooperation between national authorities

X Interoperability of databases

☐ Technical limitations in data processing

X Implementation of Eurodac and/or GDPR regulation

☐ Lack of training/information

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

X Other (please specify):

Challenges were identified in the context of this study in relation to datamanagement in the asylum procedure (since 2014). As the first step in answering this question, evaluation and other reports were examined for challenges. As the second step, in interviews with government and other stakeholders, they were asked about these and other possible challenges. As the last step, in the meeting with the focus group on 26 May 2020, EMN Netherlands discussed the challenges with the various governmental stakeholders.

The following challenge(s) emerged from the evaluation and other reports in relation to datamanagement in the asylum procedure:

Lack of human or financial resources:

- From a Security and Justice Inspectorate report from 2015[154] it became evident that to speed up the registration of asylum seekers concessions had been made to the completeness of the identification process by the organizations cooperating in the immigration process (KMar, Police, IND). The brief manner in which identification and registration took place made it difficult to answer essential questions in the assessment of asylum claims.[155] This report gave cause for the Security and Justice Secretary of State to take measures to address bottlenecks, such as the lack of experience and need for supervision among new employees, which led to a higher work pressure of more experienced staff. The quality of identification and registration was enhanced through staff briefings and issuing detailed process descriptions which were audited by the National Police. By December 2016, the Inspectorate of Security and Justice concluded that the quality assurance of the identification process was under control, recognising however that in some cases it was still difficult to establish identity (e.g. regarding undocumented asylum seekers).[156]
- A challenge mentioned by experts from the Royal Netherlands Marechaussee is making sure there is enough staff. This issue is being tackled in part by hiring new employees, not just for data management in the asylum procedure, but in general at the Royal Netherlands Marechaussee. In addition, schedules are planned 'smarter'. Essential tasks are always carried out.[157]
- A challenge mentioned by experts from the Police is to ensure that all employees obtain the level of specialized knowledge needed. Many people have left (e.g. due to a high outflow from many pensioners) and many people are joining again. A departure of staff leads to a loss of knowledge that must be gathered again. At the moment, the Police is therefore also engaged in (specialist) training to further develop this.[158]

Other:

- In a 2020 report commissioned by the Ministry of Justice and Security, it became evident that the IND's database INDiGO was not used correctly by caseworkers as data fields were frequently left empty. The following causes were identified: first, there appeared to be a lack of awareness among IND-employees that filing incomplete cases into INDiGO limits possibilities for control. Secondly,

[154] Security and Justice Inspectorate (2015). De tijdelijke (opvang) voorzieningen voor asielzoekers onder de loep. ("The temporary (reception) conditions for asylum seekers under scrutiny.") (in Dutch)
[155] Ibid., p. 5.
[156] Security and Justice Inspectorate (December 2016). Vervolgonderzoek de identificatie van asielzoekers in Nederland (''Follow-up research into the identification of asylum seekers in the Netherlands).
[157] Interview with experts from the Royal Netherlands Marechaussee on 21 April 2020.
[158] Interview with experts from the Police on 23 April 2020.

managers did not clearly instruct employees to fill in all fields, in part because they did not have an overview of the extent to which staff left fields empty. Thirdly, due to the design of INDiGO it is possible to leave certain fields empty even when (according to the manual) it is required to fill it in. The IND is currently exploring possibilities on how to address these issues. [159]

Several other challenges emerged in addition from interviews with governmental and other stakeholders concerning datamanagement in the asylum procedure*:*

GDPR and privacy:

- An expert on privacy from the IND noted that ensuring continued knowledge of privacy is an ongoing challenge within the organization. To this end, the IND has installed privacy liaisons in all directorates of the IND that answer privacy related questions for IND-employees. Additionally, an information campaign was set up to raise awareness among IND-employees in regards to privacy and data management. The daily routines and procedures are continuously reviewed and awareness is constantly being raised among colleagues. [160]
- Another challenge in this regard was mentioned by experts from the Royal Netherlands Marechaussee. They mention that there are sometimes differences between interpretation of the GDPR amongst organizations sharing information in relation to the asylum procedure and data management. This may delay processes. Moreover, an expert from the IND mentions in this regard that a lot of organizations need a lot of information, which sometimes is at odds with the rules and GDPR. [161] Due to the instalment of 'privacy officers' these issues are discussed (also amongst lawyers) so actions can be made coherently and jointly. [162]
- Experts from the Dutch Council for Refugees also mentioned a challenge in regards to the GDPR. The experts stipulate that they find that society in general become more reluctant to exchange information, which may be understandable from a privacy point of view. It appears that the GDPR is now being used to exchange even less information than before and it seems that this will delay the various procedures. The information required to continue the procedure is not being shared. This has made the GDPR a real limiting factor in some cases. [163]

Interoperability of databases

Another challenge mentioned by experts from the Ministry of Justice and Security is related to the preparation of the implementation of European regulations leading to the implementation of ETIAS and other systems and the interoperability of databases. A challenge is that some of these database use biometrical and others biographical data to establish connections. These data can lead to many potential hits and as of yet it is still unclear how it should be investigated whether these hits refer to the same person. There is a concern that national authorities will be more frequently tasked with investigating data.[164] This could be complicated further in the case of criminal inquires (Police Data Act/GDPR) and due to the fact that different systems register data in a different manner. Some systems use both biometric data and names, whereas others only use names. It is already clear how this works regarding SIS and EURODAC, but not regarding other European systems.[165]

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.

[159] Significant Public (2020), 'Onderzoek doorlooptijden IND. Definitieve rapportage' ('Research processing times IND, final report'), https://www.rijksoverheid.nl/documenten/rapporten/2020/03/03/tk-bijlage-eindrapportage-significant-onderzoek-doorlooptijden-ind, consulted October 2020.
[160] Interview with an expert on privacy from the IND on 28 April 2020.
[161] Interview with an expert from the IND on 21 April 2020.
[162] Interview with experts from the Royal Netherlands Marechaussee on 21 April 2020.
[163] Interview with experts from the Dutch Council for Refugees on 13 May 2020.
[164] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[165] This information was provided by experts from the Ministry of Justice and Security on 26 May 2020.

If not, please move to Q48.

Yes, the Netherlands has introduced major change(s)/reform(s) related to data management in the past years. Please see below.

2014

- The old version of the Municipal Personal Records Database (*Gemeentelijke Basisadministratie, GBA*) has been replaced by the new Municipal Personal Records Database (*Basisregistratie Personen, BRP*) together with the newly introduced Register of Non-Citizens (RNI).[166] The new BRP database contains the personal data of all residents of the Netherlands, and of persons abroad who have a relationship with the Dutch government. The reason for making this amendment was the following. In contrast to the GBA, the BRP makes it possible to register data of non-citizens at their own request or at the request of a designated Dutch authority. The RNI registers non-citizens who do not reside in the Netherlands or are only here for a short stay (e.g. seasonal migrants who only stay for three months). The BRP is laid down in the BRP Act. This act took effect on 6 January 2014.
- The legislative amendment of 11 December 2013 which amends the Dutch Immigration Act 2000 in relation to the extended use of biometric data by the organisations cooperating in the immigration process, which was made to further improve the establishment of a third-country national's identity.[167] As of 1 March 2014 the Dutch Immigration Act (*Vreemdelingenwet*) 2000 has been amended to facilitate an extension of the use of biometrics by the organisations concerned. The Dutch Act on Biometrics in the Immigration Process (*Wet biometrie vreemdelingenketen*) provides for an extension of the use of biometrics by organisations that cooperate in the migration process. First of all, it has been made possible to take and process a facial image and ten fingerprints of in principle all third-country nationals in all immigration law processes. Secondly, the facial image and fingerprints can be stored centrally in the third country national register and are available to all cooperating organisations.

2015

- Mid-February 2015 a final test of the BVID Kiosk (*Basisvoorziening Identificatie, BVID*) – a new facility – was run with the BVV by the Immigration and Naturalisation Service (IND), Central Agency for the Reception of Asylum Seekers (COA), the National Police, the Royal Netherlands Marechaussee, and JustID (Justice information service).[168] The BVID Kiosk integrates identification and registration processes for immigration law (asylum and supervision), criminal law and third country nationals in criminal law (VRIS) into one system. Depending on the situation and nationality of persons identified at the BVID Kiosk, the criminal law registers (VVI and SKDB) and/or immigration law registers (BVV) will be consulted and amended. From the BVID Kiosk, several registers such as Havank (IPOL's fingerprint system), EUVIS (European system for short stay visas) and Eurodac (European system for fingerprints for asylum and supervision) will also be consulted and updated if necessary. On 17 April 2015 the decision was made to proceed with the national implementation of the BVID Kiosk.

2016

- The Process Digitisation (*Keteninformatisering*) programme of the Netherlands Government was commissioned to work on an online real-time third country national profile for organisations cooperating in the immigration process. As a result, the exchange of data for the purpose of compulsory return has improved. Formerly, this data was exchanged in writing by means of the so-

[166] Government of the Netherlands (2017). *Personal Records Database (Basisregistratie Personen, BRP)* For more information, please see: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/inhoud/basisregistratie-personen-brp (in Dutch)
[167] University of Groningen (2017). *Evaluatie van de Wet biometrie vreemdelingenketen (" Evaluation of the Dutch Act on Biometrics in the Immigration Process")*. P. 7 (in Dutch).
[168] Government of the Netherlands (2015). *BVID verbindt strafrecht- en vreemdelingenketen ("ID kiosk connects criminal law and the immigration process").* For more information, please see: https://abonneren.rijksoverheid.nl/nieuwsbrieven/archief/artikel/55/1bcce598-eb49-41cf-ade9-43369d00b351/40ae9e1d-d107-4059-874a-46032ca58321 (in Dutch)

called M118 form; in 2012 this could be done online in real time by means of the Temporal Immigration Transfer Information System (*Tijdelijke Informatie Systeem Overdracht Vreemdelingen, TISOV*). This formed the basis of the information exchange which since 2016 is taking place under the name of Sigma, Sigma is used not just for M118 forms but also to exchange other data.[169] [170] [171][172] Sigma fully replaced TISOV at the start of 2017.[173]

- Since the increase in the number of applicants for international protection in 2015 and 2016, data carriers such as smartphones have been subjected to a general check (scrolling). Subsequently, based on signs during the initial identification, a selection of data carriers is further investigated. These smartphones are connected to a PC and "read". In case of suspect indications, the data carriers are turned over to the investigative authorities, outside the Identification & Registration process (I&R process), for forensic digital examination.[174] Furthermore, in 2016 the Royal Netherlands Marechaussee started undertaking the I&R Process locally, in view of increased attention for national security.[175]

2017

- As of 1 September 2017 a legislative amendment came into effect that enables asylum seekers to be registered in the BRP earlier in the process of their application for international protection (in the so-called 'BRP-straat'). Previously, registration in the BRP was only possible for admitted asylum seekers or asylum seekers who were awaiting an asylum decision for six months or more. Due to the new measure, asylum seekers can be registered in the Municipal Personal Records Database (BRP) at the earliest possible stage, on the condition that the identity has been established and the asylum seeker is expected to stay in the Netherlands for at least four months. This decision was made because both asylum seekers and the government benefit from a faster registration in the BRP. Through registration in the BRP, asylum seekers are more likely to quickly receive a citizen service number (BSN), so that they can arrange government services sooner. Three groups are excluded from the earlier registration in the BRP: third-country nationals from a safe country of origin; third-country nationals who applied for asylum elsewhere in Europe before ('Dublin'); and third-country nationals who are subjected to a security screening or an investigation for immigration enforcement.[176]

2018

- No changes/reforms to report.

2019 - 2020

- On 5 July 2018 the State Secretary of Justice and Security (Minister for Migration) announced a program with the aim of increasing the flexibility of the asylum process (*Programma Flexibilisering Asielketen).*[177] [178] [179] As part of this program, as was announced late 2018, tests were being carried out

[169] *Parliamentary Papers II, 2015 - 2016*, 19637 - no 2186 (in Dutch)
[170] Government of the Netherlands (2017). *SIGMA*. For more information, please see: https://www.zichtopdevreemdelingenketen.nl/programmaketeninformatisering/centralevoorzieningen/SIGMA/index.aspx (in Dutch)
[171] Sigma enables the structured exchange of data between the cooperating organisations. Sigma is a service that makes sure that when an organisation in the immigration process has a question about a third-country national, he or she gets one answer. The service 'consults' all connected central systems and systems of cooperating organisations. Sharing information this way makes it possible to offer the desired third country national profile to all employees, i.e. all relevant information on the third-country national the employee needs to perform his or her task.
[172] This information was provided by experts from the Ministry of Justice and Security on 29 May 2020.
[173] Inspectorate for Justice and Security, Informatieoverdracht in de asielketen, 25 November 2020, https://www.inspectie-jenv.nl/Publicaties/rapporten/2019/11/25/informatieoverdracht-in-de-asielketen, p. 19.
[174] *Parliamentary Papers (Kamerstukken) II, 2015-2016,* 19 637, no. 2187 See also the answers to AHQ on 2017.1180 – Mobile device information
[175] This information was provided by the Royal Netherlands Marechaussee on 2 June 2020.
[176] Ministry of Justice and Security, Protocol Identification and Labelling, version 10.2, p. 84; See also: Immigration and Naturalisation Service, 'Asylum Seekers registered earlier in the Municipal Personal Records Database', 29 September 2017, https://ind.nl/nieuws/Paginas/Asielzoekers-sneller-ingeschreven-in-de-Basisregistratie-Personen-(BRP).aspx, consulted October 2020; Dutch Association for Citizens' Affairs, 'Amendment Decision BRP, Waiting period registration of asylum seekers,' https://nvvb.nl/nl/nieuws/wijziging-besluit-brp-wachttermijn-inschrijving-as/, consulted October 2020.
[177] Government of the Netherlands (2018). *Brief Tweede Kamer Flexibilisering Asielketen.* For more information, see: https://www.rijksoverheid.nl/onderwerpen/migratie/documenten/kamerstukken/2018/07/05/brief-tweede-kamer-flexibilisering-asielketen (in Dutch)

with accelerated identification and registration (I&R) processes and improving coordination between the organisations cooperating in the I&R process.[180] The renewed I&R process is more focused on securing important identity-related information at the forefront of the application, which is valuable for the admission process as well as for realising return. To this end, a "Vestibule" (*Voorportaal*) is established where the asylum seeker and his/her luggage are subjected to a search, followed by identification and registration at the BVID Kiosk. During the search, attention is paid to objects such as identity documents and data carriers which may assist in establishing the identity. Furthermore, the different cooperating organisations are brought together in a multidisciplinary platform ('*regietafel*') where they process information and decide on the next steps of the application. This assessment also covers aspects related to public order and national safety; criminal records and signs of previous crimes. The I&R process was tested on different locations in the Netherlands during the fall of 2019 and was found to produce more and better information, helping cooperating partners to take decisions on the next phase of the procedure. Implementation of the renewed process was expected from mid-2020 onward.[181]

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

☒ Yes / ☐ No

Please elaborate

Yes.
SIGMA, the BVID Kiosk, the extended use of biometric data and the new Municipal Personal Records Database (BRP) have all become part of the standard operating procedure in the Netherlands.

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

☐ Yes / ☒ No

If yes, please elaborate.

No, none of the major changes under Q44 were made in relation to the introduction of the policy of ''channelling''.

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.

Information on this subject is available for the following reforms:

- The Dutch Act on Biometrics in the Immigration Process (Wet biometrie vreemdelingenketen, WBVK) and the extension of the use of biometrics by organisations that cooperate in the migration process (2014):
  An evaluation of the Dutch Act on Biometrics in the Immigration Process (Wbvk) was carried out in 2019 by the Rijksuniversiteit Groningen, commissioned by the Scientific Research and Documentation Centre of the Department of Justice (WODC). The evaluation could not provide a conclusion on whether the Wbvk had met its objectives, as it found that prior to the implementation

[178] The approach from the program is multidisciplinary. On the one hand the Dutch government is working on a redesign of (parts of) the asylum system; on the other hand, steps are being taken from existing practice to realize short term improvements.
[179] This adjustment is written under 2019/2020 since the change is still ongoing.
[180] Government of the Netherlands (2018). *Kamerbrief over stand van zaken Programma Flexibilisering Asielketen en capaciteit voor de opvang van asielzoekers.* For more information, please see: https://www.rijksoverheid.nl/onderwerpen/migratie/documenten/kamerstukken/2018/11/16/tk-stand-van-zaken-programma-flexibilisering-asielketen-en-capaciteit-voor-de-opvang-van-asielzoekers (in Dutch).
[181] Letter to Parliament of 16 June 2020 about the progress of the programme on flexibilisation of the asylum chain: https://www.rijksoverheid.nl/onderwerpen/migratie/documenten/kamerstukken/2020/06/16/tk-voortgang-programma-flexibilisering-asielketen.

of the Wbvk its goals had not been formulated clearly. However, it noted that the organisations cooperating in the immigration process all confirmed the importance of the Wbvk.[182]

- Introduction of SIGMA (2016):
  A 2019 report issued by the Inspectorate for Justice and Security on information exchange in the asylum procedure, based in part on an evaluation of SIGMA, concluded that "The scope of Sigma does not include the entire immigration chain, but is mainly aimed at preparing and realizing guided departure of a foreign national from the Netherlands. The asylum system has succeeded in developing Sigma to create an information hub for all affiliated chain partners can be consulted for a number of personal characteristics of a stranger. Some items are not available in real time and in terms of content not unambiguous and reliable." [183]
- BVID Kiosk (2015) and Renewed I&R Procedure (2016):
  The Identification and Registration Procedure as carried out by KMar and the Police has undergone a positive development since 2015, as concluded in a 2016 report issued by the Inspectorate of Justice & Security. The availability of BVID Kiosks at locations of the KMar and the Police is sufficient, and they function correctly. The quality of the identification process is now safeguarded and staff diligently follows the different steps within the procedure. The Inspectorate had no remarks on the registration stage, but for the identification stage it noted that identification can still be constrained when asylum seekers give no or limited information. This occurs for example when asylum seekers do not provide documentation. In such cases, there is limited time within the I&R Procedure to establish the identity. which means it has to be done later in the procedure.[184]

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.

The following good practices were mentioned by experts on data management in the Netherlands, which relate to the reforms mentioned under Q44:

- The implementation of the so called 'BRP-straat' and the linking of the BVV and the BRP are considered a good practice.[185] The implementation of this reform builds on a cooperation between municipalities and the organisations cooperating in the immigration process. Registration of asylum seekers in the BRP used to pose issues as municipalities do not have the same investigative capabilities as the migration authorities to confirm the identity (e.g. verifying documents, consulting databases). The IND now conducts this investigation and shares the outcome with municipalities, to enable a swift registration of the asylum seeker in the BRP. Spelling errors at registration are recognized early in the process and the foreigner's documents are issued in accordance with BRP. This prevents ambiguity and errors at a later stage in the process.
- Moreover, the implementation of the BVID Kiosk is also regarded as a good practice. Since the introduction of the BVID Kiosk, there has been a stronger streamlining of processes as well as a one-off registration and identification. In addition, it is a good tool to verify identity, with fewer errors.[186] [187]
- The Dutch Council for Refugees referred to the renewed I&R process, including its 'Vestibule' (voorportaal) and the multidisciplinary platform (regietafel), as a good practice, since these

[182] Heinrich Winter et al., Vervolgevaluatie van de Wet biometrie vreemdelingenketen, Rijksuniversiteit Groningen / WODC, 25 June 2019, https://www.tweedekamer.nl/downloads/document?id=c06701f8-bf42-4e56-8040-7840ce068530&title=Vervolgevaluatie%20van%20de%20Wet%20biometrie%20vreemdelingenketen.pdf.
[183] Inspectorate for Justice and Security, Informatieoverdracht in de asielketen, 25 November 2020, https://www.inspectie-jenv.nl/Publicaties/rapporten/2019/11/25/informatieoverdracht-in-de-asielketen, p. 30.
[184] Inspectorate for Justice and Security, Identificatie Asielzoekers in Nederland – Vervolgonderzoek naar de registratie en identificatie van asielzoekers door de politie en de Koninklijke Marechaussee, 21 December 2016, https://www.inspectie-jenv.nl/Publicaties/rapporten/2016/12/21/de-identificatie-van-asielzoekers-in-nederland---vervolgonderzoek-naar-de-registratie-en-identificatie-van-asielzoekers-door-de-politie-en-de-koninklijke-marechaussee, p. 22 and 44.
[185] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[186] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[187] Interview with experts from the Police on 23 April 2020.

developments lead to a proper and swift exchange of information during the registration phase. As a result, asylum seekers are only required to provide their data once.[188]

- Furthermore, experts from the Dutch Council for Refugees identified a good practice in the communication between cooperating organisations, i.e. the use of V-numbers when communicating about clients. This prevents cases of mistaken identity, thus safeguarding the quality of service as well as the interests of foreigners.[189]
- The following other good practices were mentioned by experts on data management in the Netherlands:
- Experts from the IND[190], the Ministry of Justice and Security[191] and the Royal Netherlands Marechaussee[192] describe the fact that all organizations cooperating in the immigration process (e.g. Police, KMar, IND) are present at one location in Ter Apel (application center) as a good practice. Because of this, employees of the different organisations can contact each other fairly easily to resolve any issues (e.g. data related issues).
- An expert from the IND[193] also mentions the digital registration form (or customer form) that is filled by the asylum seeker at the start of his/her asylum procedure as a good practice. The customer form contains a lot of information and is, in general, found to be filled in truthfully. As a result, it may be useful to verify information later on in the procedure for all partners cooperating in the immigration process.

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

    If yes, please elaborate.

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

Yes, there are on-going challenges related to data management in the asylum procedure in the Netherlands. The following challenges (also discussed in Q43) have not yet been addressed:

- In a 2020 report commissioned by the Ministry of Justice and Security, it became evident that the IND's database INDiGO was not used correctly by caseworkers as data fields were frequently left empty. The following causes were identified: first, there appeared to be a lack of awareness among IND-employees that filing incomplete cases into INDiGO limits possibilities for control. Secondly, managers did not clearly instruct employees to fill in all fields, in part because they did not have an overview of the extent to which staff left fields empty. Thirdly, due to the design of INDiGO it is possible to leave certain fields empty even when (according to the manual) it is required to fill it in. The IND is currently exploring possibilities on how to address these issues. [194]
- Experts from the Dutch Council for Refugees also mentioned a challenge in regards to the GDPR. The experts stipulate that they find that society in general become more reluctant to exchange information, which may be understandable from a privacy point of view. It appears that the GDPR is now being used to exchange even less information than before and it seems that this will delay the various procedures. The information required to continue the procedure is not being shared. This has made the GDPR a real limiting factor in some cases. [195]
- Another challenge mentioned by experts from the Ministry of Justice and Security is related to the preparation of the implementation of European regulations leading to the implementation of ETIAS and other systems and the interoperability of databases. A challenge is that some of these database use biometrical and others biographical data to establish connections. These data can

[188] Interview with experts from the Dutch Council for Refugees on 13 May 2020.
[189] This information was provided by the Dutch Council for Refugees on 26 May 2020.
[190] Interview with expert from the IND on 30 April 2020 and also mentioned in another interview with another expert from the IND on 21 March 2020 (in relation to the 'BRP-straten').
[191] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[192] Interview with experts from the Royal Netherlands Marechaussee on 21 April 2020.
[193] Interview with expert from the IND on 30 April 2020.
[194] Significant Public (2020), 'Onderzoek doorlooptijden IND. Definitieve rapportage' ('Research processing times IND, final report'), https://www.rijksoverheid.nl/documenten/rapporten/2020/03/03/tk-bijlage-eindrapportage-significant-onderzoek-doorlooptijden-ind, consulted October 2020.
[195] Interview with experts from the Dutch Council for Refugees on 13 May 2020.

lead to many potential hits and as of yet it is still unclear how it should be investigated whether these hits refer to the same person. There is a concern that national authorities will be more frequently tasked with investigating data.[196] This could be complicated further in the case of criminal inquires (Police Data Act/GDPR) and due to the fact that different systems register data in a different manner. Some systems use both biometric data and names, whereas others only use names. It is already clear how this works regarding SIS and EURODAC, but not regarding other European systems.[197]

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.

Yes, there are contingency measures in place to accelerate and/or ease the process in times of high influx of asylum seekers with regards to data management. Please see below.

- The Police can quickly open (new) locations and deliver items if necessary (e.g. BVID Kiosks). A special structure with planning options (abbreviated called 'LSGBO') is used for this. Specifically, this concerns the complete layout of new ID-facilities at potentially new locations (e.g. reception centres) and increase of capacity for the new locations.[198]

Other general measures in regards to the asylum procedure

- Aiming to manage the increased influx, the Chain-wide Operational Coordination Centre for Foreign Nationals (KOCV) was established at the time of the increased influx at the end of November 2015. The KOCV is a logistics centre in which all partners involved directly in the asylum system (IND, COA and DT&V) are represented. The decision is made to keep the KOCV open after the crisis. To learn how to respond to the increased numbers of asylum seekers in the period 2014-2016, the KOCV developed a "High influx of asylum seekers contingency plan" (*Draaiboek Hoge Instroom Asielzoekers)* in 2016. The contingency plan aims to improve the upscaling and downscaling of capacities through timely and proper coordination, so that resources can be used more efficiently and bottlenecks can be identified much faster. Key objectives are ensuring reception capacity; ensuring that the identity and place of residence of all asylum seekers is established within 24 hours; and ensuring that the registration process is completed in its entirety within 72 hours.[199]
- Currently, the organisations that cooperate in the migration process (the ministries of Justice and Security, Immigration- and Naturalization Service, COA, DT&V, DJI, Police, KMar, municipalities and civil society organizations) are developing a so called 'flexible asylum system' in a programme called *Flexibilisering Asielketen* (see also Q44). The aim of this programme is to create a system which responds more flexibly to major changes in the influx of asylum seekers. In doing so, they take into account the experiences with high influx in 2015 and 2016.[200] [201]

Additional information

Other additional information can be shared as well. Experts from the Ministry of Justice and Security mention

[196] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[197] This information was provided by experts from the Ministry of Justice and Security on 26 May 2020.
[198] Interview with experts from the National Police on 23 April 2020.
[199] Ministry of Justice and Security, High influx of asylum seekers contingency plan (*Draaiboek Hoge Instroom Asielzoekers*), Version 4.2, 13 June 2016.
[200] For more information, please see: https://www.rijksoverheid.nl/onderwerpen/migratie/programma-flexibilisering-asielketen (in Dutch)
[201] Interview with expert from the Immigration and Naturalization Service on 21 April 2020.

that data management is mostly centralised and digitalised (e.g. in databases) and therefore tasks can mostly be carried out accordingly in times of high influx.[202] An increased monitoring can be set up to see whether databases function properly in times of high influx of asylum seekers. [203]

Section 8: Conclusions [max 2 pages]

This section of the Synthesis Report will draw conclusions as to the (Member) States' existing policies, practices and case law related to the registration and data management in the asylum procedure.

With regard to the aims of this study, what conclusions would you draw from your findings reached in elaborating your national contribution? In particular, what is the relevance of your findings to (national and/or EU level) policymakers?

This study has been conducted with the objective of examining how data is managed in the asylum procedure and to identify recent developments, in particular regarding the collection of data, data sharing between asylum authorities, and safeguarding quality, as well as identify challenges and good practices that have arisen in relation to data management.

Data collection
As set out in section 1, data management in the asylum process is decentralized in the Netherlands, meaning that different information is collected by different organisations throughout the asylum process. However, there are several measures in place for different organisations to access each other's data, and to avoid duplication or deviation of data. Firstly, all asylum seekers undergo identification at the BVID Kiosk, conducted by the Police or the KMar. At this point, multiple databases are consulted to check for existing registrations. If no existing files are found, the asylum seeker is assigned a V-number and registered in the Central Shared Database with Basic Information on Applicants (BVV). The BVV can be accessed by all organisations cooperating in the asylum process through their organisations' respective systems.

Good practice
The V-number, which is connected to biometric data, is known by the asylum seeker and is used in all correspondence related to the asylum procedure. The use of the V-number can be considered a good practice for preventing duplication of files.
Challenge
With regard to the registration phase, experts mentioned the dependency on other organisations in case of technical issues with databases. Furthermore, as data is routinely scanned for duplication, "hits" with existing files often bring a need for further investigation, which can be cumbersome if the file is outdated or when the relation between files is unclear.

Data exchange
Different organisations are authorized to amend data in the BVV depending on the situation. Data changes in the BVV are visible for partner organisations, and users are asked to specify the reason for an amendment. Furthermore, cooperating organisations can "subscribe" to a certain file so that they are notified when a change has been made. Besides the BVV the Netherlands has its Municipal Personal Records Database (BRP) for all residents of the Netherlands, including third-country nationals. In the BRP, biographic data is registered. When a third-country national's personal data is registered in the BRP, a message is sent to the IND and a link with the

[202] Interview with experts from the Ministry of Justice and Security on 28 April 2020.
[203] Interview with experts from the Ministry of Justice and Security on 28 April 2020.

Good practice
As of 2017, asylum seekers can be registered in the BRP at an earlier stage. Through registration in the BRP, Asylum seekers are more likely to receive a citizen service number (BSN), so that they can arrange government services more quickly.

Challenges
Experts of the Ministry of Security and Justice voiced the concern that, as a result of new EU rules on interoperability of databases, national authorities will be more frequently tasked with investigating data. They furthermore noted a lack of clarity on how to investigate "hits" in these databases, as some use biometrical and others biographical data to establish connections.

V-number is established in the BVV. From the moment the administration number and the Citizen Service Number (BSN) are known in the BVV, changes in the BRP are automatically processed among organisations cooperating in the immigration process.

Data quality
There are several ways in which data quality is safeguarded in the asylum procedure, including through screening for duplicates upon registration and weekly sample checks by senior caseworkers. In addition, only specially authorized personnel are allowed to amend databases, and special training is provided to staff involved in data management in the asylum process. Furthermore, protocols for safeguarding of data quality have been developed and databases are designed to avoid data gaps (i.e. by making it mandatory to fill in certain fields), thus preventing errors. Moreover, through the BVID Kiosk identity-related data (including biometric data) is registered at the forefront of the asylum process This prevents the need for registering identity-related data multiple times.
Furthermore, there is also a platform for ID-experts to discuss any issues regarding data (*Ketenplatform Identiteit*).

Challenge
In recent years, concerns related to human resources (capacity, expertise) have repeatedly been voiced by the organizations cooperating in the immigration procedure, leading to a decrease in data quality and increase in work pressure. These challenges have been addressed through hiring new staff and conducting specialized trainings, as well as through staff briefings and issuing detailed process descriptions.

Good practice
In addition to the BVID Kiosk, the renewed identification and registration procedure – which has been tested since 2018 – focuses even more on registration at the very beginning, including through the so-called "Vestibule" where objects that may assist in the establishment of the identity (e.g. identity documents, data carriers) are checked upon registration at the BVID Kiosk. This development was identified as a good practice by experts for ensuring a swift and high-quality identification and registration.

Data protection
In the Netherlands, the Dutch Immigration Act regulates the use of personal data and biometrics in detail. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens,* AP) supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data. The tasks and powers of the Dutch DPA are described in the General Data Protection Regulation (GDPR), supplemented by the Dutch Implementation Act of the GDPR.
The Migration Coordination Department of the Ministry of Security and Justice employs an independent data protection official (*Functionaris Gegevensbescherming*, FG), which supervises the application of and compliance with the GDPR in as far as it concerns the facilities for which they are responsible (such as BVV and SIGMA). The organisations that fall under the Ministry of Security and Justice all have in addition to the supervising FG their own Privacy Officer that is specialized in the GDPR and/or Data Protection Act related to

their own organization. Furthermore, all systems used by the IND have undergone a Data Protection Implementation Assessment (DPIA), including INDiGO and the BVV. DPIA's have also been carried out on SIGMA and Eurodac, and internal audits have been carried out by the Police on the PSH-V database.
There are arrangements making sure that asylum seekers can access their data. They can furthermore request to modify or erase data. However, erasure is limited to some extent by the Dutch Archive Law.

Challenges
Several challenges were raised regarding data protection. Ensuring knowledge on privacy among IND employees was noted as an on-going challenge, which has been addressed through awareness-raising campaigns and by installing privacy liaisons within all directorates of the IND. Furthermore experts from the KMar noted that differences in interpretation of the GDPR may arise among organizations cooperating in the asylum process. Finally, experts from the Dutch Council for Refugees found the GDPR has decreased the willingness to share information even where it is necessary for the asylum procedure, leading to delays.

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

As mentioned in answer to question 5, these data are not available. Registering the applications (as far as executed, see question 2) is done by the National Police and the Dutch Royal Marechaussee in their own data systems. No statistics are ever made about these registrations.

Annex 1.2. Number of lodged asylum applications

data management_statistic