Management of the data in asylum procedures

EMN
European Migration Network   POLAND

Management of the data in asylum procedures

Report of the European Migration Network in Poland

Warsaw 2020

Ministerstwo
Spraw Wewnętrznych
i Administracji

Project is co-funded by the European Union's Asylum, Migration and Integration Fund

EMN
European Migration Network
POLAND

4

Table of contents

Definitions

'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."[1]

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

'Data management' is understood as the administrative process that includes all operations that are performed on data or on sets of data, through automated or other means, such as collection, recording, storage, retrieval, use, disclosure by transmission, dissemination or erasure.[2]

'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.[3]

'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.[4]

'Registering an asylum application': Record the applicant's intention to seek protection.[5] 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

---

1. UNHCR, Discussion Paper *Fair and Fast – Accelerated and Simplified Procedures in the European Union*, July 2018, pp. 8f. Available at: https://www.refworld.org/pdfid/5b589eef4.pdf
2. Definition for the purposes of this study.

3. Article 6 (2, 3, 4) of Directive 2013/32/EU (Recast Asylum Procedure Directive).
4. Article 2 of Directive 2011/95/EU (Recast Qualification Directive).
5. EASO, presentation, 9th Consultative Forum, 12th November 2019, Brussels.

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.[6]

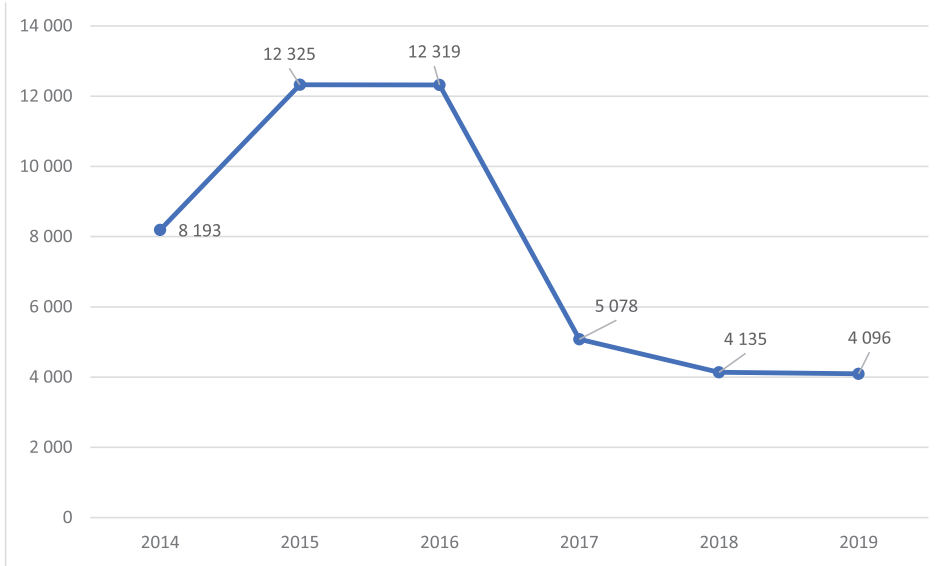**'Procedure for international protection'**: Set of measures described in the Directive 2013/32/EU (Recast Asylum Procedures Directive) which encompasses all necessary steps for granting and withdrawing international protection starting with making an application for international protection to the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

[6.] Article 6(1) of Directive 2013/32/EU (Recast Asylum Procedure Directive).

Introduction

CHART 1. Number of registrations of asylum applications (2014–2019)

SOURCE: own elaboration based on data of the Office for Foreigners

Poland is not one of the countries where foreigners apply for international protection in large numbers. Looking at the statistical data, it can be noticed that the number of immigrants applying for protection is decreasing every year – from 12,325 applications in 2015 to 4,096 in 2019. Poland has not introduced changes with regard to data management in the case of applications related to the asylum procedure as a result of the COVID-19 pandemic.

The main body responsible for accepting applications in the field of international protection in Poland is the Border Guard. Due to the fact that one authority is responsible for all stages of the asylum procedure, the submission of the application, its registration and formal submission are the only stage in the procedure under consideration. These stages are separated only when the Border Guard authority cannot accept the application at the moment or the foreigner cannot appear in person at the Border Guard post. Only with regard to examining applications, the competent authority is the Office for Foreigners in the first instance and the Refugee Council in the second instance. In practice, the data collected during individual stages of the international protection procedure are collected by the Border Guard (national databases Pobyt v. 2 and the Register of Refugee Proceedings) and the Office for Foreigners, which has access only to the Pobyt v.2 database.

The Border Guard carries out cross-checkings: checks the foreigner's data in several databases. Foreigners are informed about the processing of their personal data. Both of these activities are performed only at the stage of formal submission of applications

for international protection. Information on data quality is not collected in Poland.

The only change regarding data management in the last 6 years was the adaptation of the rules for the processing of personal data to the requirements of the GDPR Regulation on the protection of personal data – including the introduction of the obligation to inform about the rules for processing personal data of persons whose data is processed. There were no problems in this regard. Due to the low number of submitted applications for international protection, Poland does not apply contingency measures to accelerate or facilitate the process in relation to data management.

1

The asylum procedure

Submitting an application, registering and formally submitting an application essentially follow the same step. Such a state has been achieved thanks to the fact that the authorities of the Border Guard can be designated as the body to which the willingness to apply for international protection can be submitted and which is competent for accepting formal applications. It should be emphasized at this point that the Border Guard posts are located not only on the border, but throughout the country.

When a foreigner declares his willingness to submit an application, he or she receives relevant instructions on the procedure, fingerprints are taken, a photograph is taken, and then a formal application is completed. This request is registered in the system. A document is issued to the foreigner (a temporary foreigner's identity certificate).

Only if the Border Guard authority is unable to accept the application at a given moment (e.g. lack of availability of the necessary interpreter), or the foreigner cannot appear in person at the Border Guard facility (e.g. due to staying in a hospital or prison), is admitted first, a declaration of intention to submit an application, and then, within 3 working days, a formal application for international protection. In this case, however, also the registration of the application takes place simultaneously with its formal adoption.

The so-called Dublin cases are handled separately. If in the content spoken by a foreigner when accepting the application for international protection there are elements that may indicate premises for the transfer of the foreigner under the Dublin III Regulation, the Border Guard writes "D" in the foreigner's documentation file, which is information for the Office for Foreigners that the case must first be referred to the appropriate department dealing with Dublin proceedings.

If, for reasons attributable to the Border Guard authority, it is not possible to accept the application for international protection or if the foreigner cannot appear in person at the seat of the Border Guard authority, the application for international protection is accepted and registered immediately, but not later than within 3 working days from the date of acceptance of the declaration of intention to submit such an application, and in the event of a mass influx of foreigners to the territory of the Republic of Poland in order to obtain international protection – within 10 working days.

As a rule, after a foreigner declares his will to submit an application, such an application is accepted immediately. A small percentage is the acceptance of the declaration and then the application. Therefore, consider that the average period in days is 0 (same day).

TABLE 1. Days from lodging until first time decision

Year	Average days
2014	200
2015	118
2016	86
2017	221
2018	247
2019	152

SOURCE: data of the Office for Foreigners

As can be seen from the table above, in 2014-16 there was a decrease in the number of days from submitting the application to its first instance decision. After an increase in 2018 and 2019, the average period starts to decline again.

TABLE 2. Authorities involved in and responsible for the asylum procedure

Type of Authority	Name of the authority involved in making an application	Legally competent for registering an asylum application	Legally competent for lodging an asylum application	Legally competent for examining an asylum application
Border Police	Border Guard	Border Guard	Border Guard	
(Branch) office for Refugees				Head of The Office for Foreigners (1st instance); Council for Refugees (2nd instance)

SOURCE: data of the Border Guard and the Office for Foreigners

Polish Border Guard is competent for making, registering and lodging asylum applications. The institution responsible for examining applications is the Office for Foreigners. In the event of an appeal against the decision of the office, the competent authority is the Office for Foreigners in the first instance, and the Council for Refugees in the 2nd instance. Such a division accelerates the process from submitting an application to issuing a decision. The Border Guard is a more technical institution, although it must also check the correctness of submitting the application, which is the first and most important step in the asylum procedure. The Office for Foreigners checks the application in terms of its merits and Council for Refugees issues decisions only when foreigners appeal against the decision of the Office for Foreigners.

TABLE 3. Type of information and organization during the asylum procedure at the different phases

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
NAME					
• current name	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
• birth name	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
• previous name(s)	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
• pseudonim literacki					
• imiona religijne	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
• inne imiona	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU
SEX	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	Pobyt v.2 RPU
BIOMETRIC DATA					
• photo	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Camera, photo taken by a forensics technician	in database (1) and on paper (2)	Pobyt v.2 RPU
• fingerprints (which fingers, rolled or pressed fingerprints)	10 fingers rolled and hands pressed	Border Guard – at Border Guard posts (1, 2)	Live Scanner (in the absence of the device – ink techniqued on the dactyloscopic card)	in database (1) (on paper when ink technique is performed	Eurodac AFIS
• iris scan					
• other					
EYE COLOUR	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Data recording by a forensics technician	in database (1) and on paper (2)	RPU Pobyt v.2
HEIGHT	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Measurement by a forensics technician	in database (1) and on paper (2)	RPU Pobyt v.2
DATE OF BIRTH	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
CITIZENSHIP(S)	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
COUNTRY OF ORIGIN	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
PLACE OF BIRTH					
• town	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
• region	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
• country	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	RPU Pobyt v.2
• other					
DATE OF ARRIVAL IN THE (MEMBER) STATE	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	Pobyt v.2 RPU
LAST PLACE OF RESIDENCE IN THE COUNTRY OF ORIGIN	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	Pobyt v.2 RPU
LAST PLACE OF RESIDENCE BEFORE ENTRY IN THE (MEMBER) STATE					
CONTACT DETAILS					
• phone number	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2)	in database (1) and on paper (2)	Pobyt v.2
• email address					
• current address	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2); oral (interview via phone/ videocall) (3)	in database (1) and on paper (2,3)	Pobyt v.2 RPU
• other					
CIVIL STATUS	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	Pobyt v.2
ACCOMPANIED BY:					
• spouse or civil partner	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	Pobyt v.2 RPU

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
• children	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	Pobyt v.2 RPU
• parents	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	Pobyt v.2 RPU
• other relatives					

CZŁONKOWIE RODZINY W PAŃSTWIE (CZŁONKOWSKIM)

1. Categories of data collected	2.	3.	4.	5.	6.
• name	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	RPU
• residency	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	RPU
• citizenship	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	RPU
• other					
FAMILY MEMBERS IN ANOTHER (MEMBER) STATE	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	RPU
CLOSE RELATIVES IN THE (MEMBER) STATE	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2,3)	RPU
CLOSE RELATIVES IN ANOTHER (MEMBER) STATE	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2) ; oral (3)	in database (1) and on paper (2,3)	RPU

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
HEALTH STATUS					
• specifics on health status	1/2 (combined phases)	Border Guard – at Border Guard posts (1, 2)	Interview and filling out the application – general information provided by the foreigner (1, 2)	in database (1) and on paper (2)	RPU
• reference that a general health check has been carried out	2	The medical entity conducting the medical examination	Medical examination performed after the application was approved	on paper in the patient's chart (2)	
• other					
EDUCATION					
• school attendance	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
• academic studies	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2); Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
• trainings	3	Office for Foreigners (3)	Oral (3)	On paper (3)	
• apprenticeships	3	Office for Foreigners (3)	Oral (3)	On paper (3)	
• non-formal work experience	3	Office for Foreigners (3)	Oral (3)	On paper (3)	
• other	3	Office for Foreigners (3)	Oral (3)	On paper (3)	
Language skills	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
Profession	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
Criminal record	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
Financial resources					

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
SUPPORTING DOCUMENTS					
• passport	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
• travel document	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
• other		Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	RPU
Reasons for fleeing	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	RPU
Reasons for not wanting to be returned to the competent Member State as part of a Dublin procedure	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	
Previous applications	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	Pobyt v.2 RPU
Information on the route taken	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	RPU
Information on exclusion grounds	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2) ; Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	RPU
Religious affiliation	1/2 (combined phases); 3	Border Guard – at Border Guard posts (1, 2);Office for Foreigners (3)	Interview and filling out the application (1, 2, 3)	in database (1) and on paper (2, 3)	RPU

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)	3. Which organization collects this information in each of the different phases?	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	5. Where is this particular category of data /biometric data stored?	6. If applicable, please specify the name of the database(s)
VULNERABILITIES					
• Unaccompanied minor	1/2 (combined phases); 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (1, 2, 3)	in database (1) and on paper (2, 3)	RPU Pobyt v.2
• Pregnant	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Disabilities	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Elderly	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Single parent with minor child(ren)	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Victims of human trafficking	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Mental disorders	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Victims of torture, physical or sexual violence	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Other	2, 3	Border Guard – at Border Guard posts (2); Office for Foreigners (3)	Interview (2, 3)	in database (1) and on paper (2, 3)	
• Information on completed military service	1/2,	Border Guard (1, 2)	Filling out an application (1, 2)		

SOURCE: data of the Border Guard and the Office for Foreigners

As can be deduced from the table above, there are 2 main institutions responsible for collecting information in each of the phase of asylum procedure: Border Guard (phase of registering and lodging) and Office for Foreigners (examination phase). Very rarely do other organs participate in this process – as in the case of health status there is a medical entity conducting the medical examination.

TABLE 4. Data management during the asylum procedure

Baza danych	Opis / informacje na temat bazy danych (proszę wskazać, czy jest to baza regionalna, krajowa czy europejska).	Organy krajowe, które posiadają dostęp do tej bazy danych lub dostęp do danych w niej zawartych			Dane udostępniane innym państwom członkowskim (poza danymi udostępnianymi przez państwa (członkowskie) za pośrednictwem unijnych baz danych, np. Eurostat, VIS, SIS)	
		Nazwa organu/ organizacji	Etap procedury	Cel	Rodzaj danych	Cel
Pobyt v.2	Baza krajowa	Straż Graniczna Urząd do Spraw Cudzoziemców Rada ds. Uchodźców, sądy administracyjne	Rejestracja wniosku, Rozpatrzenie wniosku	Rejestracja i rozpatrzenie wniosku	x	x
RPU (Rejestr Postępowań Uchodźczych)	Baza krajowa	Jeden z modułów wewnętrznej bazy Straży Granicznej "System Obsługi Cudzoziemców"	Straż Graniczna	Przyjmowanie i rejestracja wniosku	Rejestracja danych i wygenerowanie wniosku uchodźczego	Nie udostępniane

SOURCE: data of the Border Guard and the Office for Foreigners

There are two national databases, where data during the asylum procedures are proceed: The Pobyt System and the Register of Refugee Proceedings (RPU).

2

Lodging an asylum application

After submitting the application, the Border Guard checks the foreigner each time in the internal databases of the Border Guard, in the national Information System Pobyt v.2, in the National Police Information System, as well as in SIS, in VIS (both alphanumeric and biometric data) and in the database.

The Pobyt system is the main ICT tool used in the Office for Foreigners. The system maintains a national set of registers for the registration and list of foreigners referred to in Chapter 3, Section X of the Act of 12 December 2013 on foreigners. Information on applications for international protection, administrative decisions issued in these matters, lodged appeals, decisions of the Council for Refugees and documents issued to foreigners are collected and processed in the system. At the same time, the system collects and processes information on administrative proceedings related to the legalization of the stay of foreigners, which enables the creation of the entire history of the foreigner's stay, with the exception of matters related to visas issued by consulates. The Pobyt v. 2 system is also connected to the Schengen Information System (SIS II) and enables authorized users to perform checks and entries also in this database.

The system enables, among others:

• completing applications regarding the legalization of stay in an electronic version, with the possibility of transferring data from these applications to the appropriate registers / records kept in the Pobyt v.2 System;

• monitoring the status of administrative matters;

• sending inquiries in electronic form to competent authorities;

• informing about the provisions and procedures regarding the legalization of stay and the above-mentioned migration authorities in order to provide complete information on the process of handling legal migration;

• making stamp duties, necessary to be made in the course of proceedings related to the legalization of stay in Poland, which will contribute to easier monitoring of payments made by foreigners, in the above-mentioned range.[7]

The National Police Information System (KSIP) – a central collection of information about suspected offenses prosecuted under public prosecution, persons wanted or trying to hide their identity, as well as about lost or stolen property.

SIS (Schengen Information System) is the largest database in Europe in which the legal categories of data of persons and objects, searched for and entered into the system by the Schengen countries, are processed. The uniqueness of this system is based on the tasks it performs and its territorial scope. Building such an IT tool, taking into account the specific, technical solutions of its users, as well as respecting their legislation, makes it one of the greatest achievements of the European Union. A consequence of the EU enlargement in recent years was the inclusion of new countries in the zone, due to the fact that the technical infrastructure of the SIS made it impossible to switch them to the existing system, anticipating this situation long before this decision was taken, it was decided to replace SIS with the new second generation Schengen Information System (SIS II). Ultimately, all Member States were required to introduce SIS II, which was to be a much more functional system.

An additional reason for launching the new generation SIS II were also limitations as to the possibility of processing such a large amount of data by SIS 1+ (modernized SIS I system). It should be emphasized that the changes to the SIS will not cover the system's objective of ensuring a high level of security in the area of freedom, security and justice of the European Union. The basis for the creation of the second generation Schengen Information System (SIS II) are two documents issued on the basis of Title VI of the EU Treaty, i.e. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the System Second Generation Schengen Information System (SIS II) (hereinafter referred to as the Regulation) and Council Decision 2007/533 / JHA of 12 June 2007 on the establishment, operation and use of the Second Generation Schengen Information System (SISII) (hereinafter the Decision). The Regulation and the Decision replaced

---

7. https://udsc.gov.pl/urzad/projekty-i-programy/projekty-realizowane-przez-urzad/w-realizacji/modernizacja-pobytu-modul-obslugi-spraw/

Art. 92-119 of the Convention Implementing the Schengen Agreement and decisions and declarations of the Schengen Executive Committee regarding the SIS. The provisions of the Schengen acquis and Community law concerning the SIS were implemented into the Polish legal order by the Act of August 24, 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, Journal Journal of Laws No. 165, item 1170 as amended (hereinafter referred to as the Act). The Act comprehensively regulates the rules and manner of participation in SIS II[8].

The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. The main purposes of VIS are:

- Facilitating checks and the issuance of visas: VIS enables border guards to verify that a person presenting a visa is its rightful holder and to identify persons found on the Schengen territory with no or fraudulent documents. Using biometric data to confirm a visa holder's identity allows for faster, more accurate and more secure checks. The system also facilitates the visa issuance process, particularly for frequent travellers.
- Fighting abuses: While the very large majority of visa holders follow the rules, abuses can also take place. For instance, VIS will help in fighting and preventing fraudulent behaviours, such as "visa shopping" (i.e. the practice of making further visa applications to other EU States when a first application has been rejected).
- Protecting travellers: Biometric technology enables the detection of travellers using another person's travel documents and protects travellers from identity theft.
- Helping with asylum applications: VIS makes it easier to determine which EU State is responsible for examining an asylum application and to examine such applications.
- Enhancing security: VIS assists in preventing, detecting and investigating terrorist offences and other serious criminal offences.[9]

The Border Guard gives the foreigner a relevant instruction after submitting the application for granting international protection by her/him. Written information is currently available in Polish, Russian, Ukrainian and English. Translations into Spanish, Arabic, Chinese, Vietnamese are expected. If a given language version is not available, the information is translated by a translator appointed for the purpose of accepting the application for international protection. The costs of the interpreter are covered by the Border Guard. Border Guard officers are provided with general training in the area of data management and in the area of processing of personal data (including data relating to international protection).

8. https://www.policja.pl/pol/sirene/sis/12473,Co-to-jest-System-Informacyjny-Schengen-SIS.html

9. https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en

3

Data management
in the asylum procedure

One of the important part of data management is data protection. Please find below information of Border Guard for persons from whom an application for granting international protection has been accepted. It describes the supervision mechanism for data protection supervision of the personal data collected during the asylum procedure in Poland.

"Dear Madam/Sir

in connection with the entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as "RODO", we would like to inform you that in terms of the processing of personal data due to the acceptance of an application for granting international protection.

1. The controller of personal data is the Commander in Chief of the Border Guard (Komendant Główny Straży Granicznej):
   - address: Al. Niepodległości 100, 02-514 Warsaw
   - phone: +48 22 500 40 00
   - e-mail: gabinet.kg@strazgraniczna.pl
2. The supervision over the proper processing of personal data in the Border Guard is exercised by the Data Protection Inspector (Inspektor Ochrony Danych):
   - Director of the Information Protection Bureau of the Border Guard Headquarters (Dyrektor Biura Ochrony Informacji Komendy Głównej Straży Granicznej)
   - address: Al. Niepodległości 100, 02-514 Warsaw
   - e-mail: boi.kg@strazgraniczna.pl
   - phone: + 48 22 500 40 35
3. The person to be contacted on data protection is
   - the Head of the Information Protection Department (Naczelnik Wydziału Ochrony Informacji) of the.. Border Guard Regional Unit (......................... Oddział Straży Granicznej)
   - address: ....
   - e-mail: ....
   - phone: ....

4. The purpose and legal basis for processing personal data.
   The purpose of data processing is the acceptance of an application for granting international protection.
   The data shall be processed on the basis of:
   - Article 24 section 1 or section 2 of the Act of 13 June 2003 on granting protection to foreigners within the territory of the Republic of Poland (Journal of Laws of 2019, item 1666),
   - Article 120 point 1 in connection with article 119 section 1 point 1 of the Act of 13 June 2003 on granting protection to foreigners within the territory of the Republic of Poland (Journal of Laws of 2019, item 1666).
5. The recipients of personal data.
   In the case of the acceptance of an application for granting international protection., information in this respect shall be transferred to the Head of Aliens' Affairs Office.
   Your personal data may be transferred to public authorities and entities performing public tasks or acting on behalf of public authorities, to the extent and for the purposes that result from the provisions of generally applicable law.
6. Transfer of personal data to a third country or international organizations.
   Personal data may be transferred to third countries or to international organizations under provisions of the law or with your consent.
7. Time for which personal data will be stored in the Border Guard.
   Data shall be stored for the period of time necessary to achieve the purpose of the processing, not longer than 10 years, counting from the time the information is entered in the filing system and, where an information entry is modified, from the last modification of that entry.
8. Rights of natural persons whose personal data are processed by the Border Guard.
   In connection with the processing of personal data by the Border Guard, you have the following rights:
   a) the right of access to personal data, including the right to obtain a copy of such data when the data subject shows a legal interest;
   b) the right to request the rectification (correction) of personal data;

c) the right to request the deletion of personal data (so-called 'right to be forgotten'), when:
- the data is no longer necessary for the purposes for which it was collected or otherwise processed,
- personal data is processed unlawfully,
- personal data must be deleted in order to comply with the legal obligation.

9. Right to lodge a complaint with the supervisory authority.
    In case of obtaining information about unlawful processing of personal data in the Border Guard, you have the right to lodge a complaint with the supervisory body competent in matters of personal data protection (President of the Office for Personal Data Protection Prezes Urzędu Ochrony Danych Osobowych, 2 Stawki Street, 00-193 Warsaw).

10. Profiling.
    Your personal data are not profiled and decisions are not made automatically.
11. Obtaining personal data from other entities.
    Data are not obtained from other entities[10]".

The only challenge that Poland faced during the last years was implementation of GDPR regulation. Adjustment of the rules for the processing of personal data to the requirements of the GDPR Regulation on the protection of personal data – including the introduction of an obligation to inform the persons whose data is processed about the rules for the processing of personal data.

---

10. Information for persons from whom an application for granting international protection has been accepted, Border Guard, 2020.

4

Conclusions

Russia, Ukraine and Tajikistan are the 3 countries from which the most applications for international protection in Poland originate. Russians of Chechen nationality submit the most applications. Poland is characterized by low recognition – international protection is granted to approx. 7% of people who submitted applications. This is probably one of the reasons for the falling number of applications for protection. In 2015, there were 12,325 applications submitted, in 2017 – 5,078, and in 2019 only 4,096. The COVID-19 pandemic caused a further reduction in the interest of applicants in Poland. A positive phenomenon is the shortening of the period for processing applications by the Office for Foreigners – in 2018 it was 247 and in 2019 it was already 152.

Data management as part of the asylum prcedure, i.e. all operations carried out on data or data files in an automated or other way, e.g. collecting, recording, storing, downloading, using, disclosing by sending, distributing or deleting is not common in Poland. Cross-checking of data understood as checking foreigner's data in various databases takes place only at the stage of formal application submission and is carried out by the Border Guard. When accepting the application, the Border Guard each time checks the foreigner in the internal databases of the Border Guard, in the national Information System Pobyt v.2, in the National Police Information System, as well as in SIS, in VIS (both alphanumeric and biometric data) and in the database Interpol I-24/7. There is "channeling" in the area of data management – tah Dubline procedure's cases are handled separately. Data on the number and nationality of applicants for international protection as well as on the number of positive and negative applications are processed by the Office for Foreigners. On their basis, reports are prepared as well as publicly available studies, thanks to which one can obtain detailed information on statistics concerning international protection in Poland.

When it comes to the protection of personal data, the foreigner gets acquainted with information about it in writing. The information is available in Polish, Russian, Ukrainian and English. If a given language version is not available, the information is translated by the translator appointed for the purpose of accepting the application for international protection. The costs of the interpreter are covered by the Border Guard.

A kind of challenge that Poland has faced in the last 6 years has been to adapt the rules of personal data processing to the requirements of the GDPR Regulation on the protection of personal data – including the introduction of an obligation to inform about the rules for the processing of personal data of persons whose data is processed. However, it did not concern the change of the "channeling" system and it covered all institutions in Poland that processed personal data. Currently, no challenges have been identified with the management of data in the international protection procedure. Due to the decreasing number of applications for protection, no changes to the procedures in the analysed scope are expected.