

2024

ROMANIA
MINISTRY OF INTERNAL AFFAIRS
GENERAL INSPECTORATE OF THE BORDER POLICE



**GUIDELINES FOR THE EXERCISE OF THE RIGHTS
BY PERSONS WHOSE PERSONAL DATA ARE
PROCESSED IN THE EUROPEAN ENTRY/EXIT
SYSTEM (EES) - REGULATION (EU) 2017/2226**

This guide provides essential information, according to Regulation (EU) 2017/2226 (Entry/Exit System - EES) and the General Data Protection Regulation (GDPR), about access, rectification, deletion and restriction of data processing, as well as about the procedures for exercising these rights in the Entry/Exit System (EES).

Table of contents

| | |
|--|----|
| 1. ENTRY/EXIT SYSTEM (EES) INTRODUCTION | 2 |
| 1.1. General information about the personal data controller: | 2 |
| 1.2. General information on the Entry/Exit System (EES)..... | 2 |
| 1.3. Data available in the Entry/Exit System (EES)..... | 3 |
| 1.3.1. For Third Country Nationals (TCN) subject to visa requirement | 3 |
| 1.3.2. For TCN exempt from visa requirement | 4 |
| 1.4. Entry/Exit System (EES) Objectives | 4 |
| 1.5. Access to the Entry/Exit System (EES) | 5 |
| 2. RIGHTS OF DATA SUBJECTS WHOSE DATA ARE PROCESSED IN THE ENTRY/EXIT SYSTEM (EES)..... | 6 |
| 2.1 Right to information..... | 7 |
| 2.2. Right of access to data | 9 |
| 2.3. The right to rectification, completion and erasure of personal data, and of restriction of the processing thereof | 9 |
| 2.3.1. Right to rectification and completion | 9 |
| 2.3.2. Right to erasure (right to be forgotten) | 9 |
| 2.3.3 Right to restriction of processing..... | 9 |
| 2.3.4. Exceptions (Article 52 of EES Regulation) | 10 |
| 2.4. Right to Appeal..... | 11 |
| 2.4.1. The right to lodge a complaint with a supervisory authority (art.77 of GDPR and art. 20 of Law no. 300/2022)..... | 11 |
| 2.4.2. The right to go to Court (art. 79 of GDPR) | 11 |
| 3. PROCEDURE FOR EXERCISING RIGHTS | 11 |
| 3.1. Exercise of the rights of the data subject by representation..... | 12 |
| 4. TERMS | 12 |
| 5. RESTRICTIONS AND EXCEPTIONS | 12 |
| 5.1. Restrictions | 12 |
| 5.2. Exceptions | 13 |
| 6. CONTACT DETAILS..... | 13 |
| 7. DEFINITIONS..... | 14 |
| 8. TEMPLATE FOR EXERCISING RIGHTS..... | 16 |
| 8.1.Application for exercising the right of access..... | 16 |
| 8.2. Application for exercise of the right to rectification/completion..... | 17 |
| 8.3. Request to exercise the right to erasure | 18 |

1. ENTRY/EXIT SYSTEM (EES) INTRODUCTION

1.1. General information about the personal data controller:

The Romanian Border Police (RBP) is part of the Ministry of Internal Affairs (MIA) and is the specialized institution of the state exercising its attributions regarding the supervision and control of the crossing of the state border, preventing and combating illegal migration and acts specific to cross-border crime committed in the area of competence, observing the legal regime of the state border, passports and foreigners, ensuring the interests of the Romanian state on the inner Danube, including the Macin arm and the Sulina canal located outside the border area, in the contiguous area and in the exclusive economic zone, observing public order and tranquility in the area of competence, according to law.

In accordance with the provisions of [G.E.O nr. 104/2001](#) *on the organization and functioning of the Romanian Border Police*, as subsequently amended and supplemented, the RBP activity constitutes a public service and is carried out in the interest of the person, the community and in support of state institutions, exclusively on the basis and in the execution of law.

The General Inspectorate of the Border Police (GIBP) is the central unit of RBP, with legal personality and territorial competence for the entire area of responsibility of the border police, which exercises the management and is responsible for the entire activity of the border police, carries out activities of investigation of particularly serious crimes circumscribed to organized crime, illegal migration and cross-border crime committed in the area of territorial competence of RBP, as well as any other powers given to it by law.

GIBP is a personal data controller, in accordance with Article 4 point 7 of [Regulation \(EU\) 2016/679](#) *of the European Parliament and of the Council 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 (GDPR)*.

Also, according to art. 17 of Law no. 300/2022 *establishing the organizational framework for the national operationalization of the Entry/Exit System and the European Travel Information and Authorization System, in application of the provisions of Article 39 paragraph (1) of EES Regulation, **the General Inspectorate of the Romanian Border Police has been designated as a personal data controller for the data processing carried out within EES and ETIAS systems***, respectively for the performance of the specific tasks of the ETIAS National Unit.

1.2. General information about the Entry/Exit System (EES)

The Entry/Exit System (EES) is an automated IT system for registering travellers from third countries, both holders of short-stay visas and visa-exempt travellers, each time they cross an external EU border. The system will record the person's name, type of travel document, biometric data (***fingerprints and facial images captured***), as well as the date and place of entry and exit, in full respect of fundamental rights and data protection. The system will also record refusals of entry.

The EES will replace the current, time-consuming manual passport stamping system, which does not provide reliable border transit data and does not allow systematic detection of people who have exceeded the maximum length of authorised stay (*travellers who have exceeded the maximum length of authorised stay*).

The EES will help prevent illegal migration and protect the security of European citizens. The new system will also help bona fide third-country nationals to travel more easily while more effectively identifying overstayers as well as cases of document and identity fraud. In addition,

the system will allow a wider use of automated border control checks and self-service systems, which are faster and more comfortable for the traveler.

1.3. Data available in the Entry/Exit System (EES)

Personal data is processed in EES whenever a third-country national crosses the state border. The types of data that can be collected and processed in EES are those indicated in Articles 16, 17, 18, 19 and 20 of [Regulation \(EU\) 2017/2226](#).

The EES is an information system that is based on the **collection of alphanumeric data** (such as name, surname, date of birth etc.) and **biometric data** (facial image and four fingerprints) as required by Articles 15-20 of Regulation (EU) 2017/2226.

The following data may be collected by EES:

1.3.1. For Third Country Nationals (TCN) subject to visa requirement:

- surname (surname); first name (s); date of birth; nationality (ies); sex;
- the type and number of the travel document (s) and the three-letter code of the issuing country of the travel document (s);
- the expiration date of the validity of the document or travel documents;
- real-time facial image or electronically extracted from the chip of the electronic machine-readable travel document;
- date and time of the exit;
- the border crossing point at entry/exit and the authority that authorised the entry/exit;
- where applicable, the status of that third-country national indicating that he or she is a third-country national who:
 - i. is a family member of a Union citizen to whom Directive 2004/38/EC applies or a third-country national enjoying the right of free movement equivalent to that of Union citizens under an agreement concluded between the Union and its Member States, on the one hand, and a third country, on the other; and
 - ii. does not hold a residence permit under Directive 2004/38/EC or a residence permit under Regulation (EC) 2002/1030.
- where applicable, the number of the short-stay visa sticker, including the three-letter code of the issuing Member State, the type of short-stay visa, the expiry date of the maximum duration of stay authorised by the short-stay visa, which must be updated at each entry, and the expiry date of the short-stay visa;
- at the first entry on the basis of the visa, the number of entries and the authorised period of stay as indicated on the visa sticker;
- where applicable, information indicating that the short-stay visa was issued with limited territorial validity pursuant to Article 25 (1) (b) of Regulation (EC) 2009/810;
- for Member States that do not yet fully apply the Schengen acquis but operate the EES, as appropriate, a notification indicating that the third-country national has used a national short-stay visa for entry;
- if they have been identified as overstaying;
- whether they benefit from a Member State's national facilitation programme;
- refusal of entry, as appropriate, as well as the reasons for the decision;
- data on the revocation, cancellation or extension of the short-term residence permit or visa, as well as the reasons for the decision;
- data in case of reversal of the presumption that a third-country national does not meet the conditions regarding the duration of authorised stay.

1.3.2. For TCN exempt from visa requirement

- surname (surname); first name (s); date of birth; nationality (ies); sex;
- the type and number of the travel document (s) and the three-letter code of the issuing country of the travel document (s);
- the expiration date of the validity of the document or travel documents;
- real-time facial image or electronically extracted from the chip of the electronic machine-readable travel document;
- fingerprint data from the right hand, where available, and otherwise corresponding fingerprint data from the left hand; the fingerprint data is of sufficient resolution and quality to be used in automated biometric matching;
- where relevant, whether it benefits from a Member State's national facilitation programme;
- date and time of the exit;
- the border crossing point at entry/exit and the authority that authorised the entry/exit;
- where applicable, the status of that third-country national indicating that he or she is a third-country national who:
 - i. is a family member of a Union citizen to whom Directive 2004/38/EC applies or a third-country national enjoying the right of free movement equivalent to that of Union citizens under an agreement concluded between the Union and its Member States, on the one hand, and a third country, on the other; and
 - ii. does not hold a residence permit under Directive 2004/38/EC or a residence permit under EC Regulation No. 1030/2002.
- if they have been identified as overstaying;
- refusal of entry, as appropriate, as well as the reasons for the decision;
- data on the revocation, cancellation or extension of the short-term residence permit, as well as the reasons for the decision;
- data in case of reversal of the presumption that a third-country national does not meet the conditions regarding the duration of authorised stay.

1.4. Entry/Exit System (EES) Objectives

By recording and storing data in the EES, as well as by providing Member States access to such data, the objectives of the EES, according to Article 6 of [Regulation \(EU\) 2017/2226](#), are the following:

- increase the effectiveness of border checks by calculating and monitoring the duration of authorised stay on entry and exit of third-country nationals who are admitted for a short-term stay;
- support the identification of third-country nationals who do not, or no longer, fulfil the conditions for entry or short-term stay on the territory of the Member States;
- to allow the identification and detection of persons who have overstayed their authorised stay and to allow the competent national authorities of the Member States to take appropriate measures;
- allow electronic verification in the EES of refusals of entry;
- to allow the automation of border checks carried out on third-country nationals;
- to allow the visa authorities to have access to information on the lawful use of previous visas;
- inform third-country nationals of the duration of their authorised stay;
- to collect statistical data on entries and exits, refusals of entry and situations of overstay of authorised duration of stay in respect of third-country nationals in order to improve the assessment of the risk of overstay of authorised duration of stay and to support the development, at Union level, of evidence-based migration policies;
- to combat identity fraud and misuse of travel documents.

1.5. Access to the Entry/Exit System (EES)

Access to the EES is limited for the **competent national authorities**, as border, immigration and visa authorities. Pursuant to art. 3 of Law no. 300/2022, the competent authorities in Romania with the right of access to EES are:

- ❖ The **Romanian Border Police** subordinated to the Ministry of Internal Affairs, as border authority and responsible for immigration and visas, for the purposes provided for in Articles 23, 24, 26 and 27 of EES Regulation;
- ❖ **The National Visa Center** within the Ministry of Foreign Affairs and the diplomatic missions and consular offices of Romania, as authorities responsible for visas, for the purpose provided for in Article 24 of EES Regulation;
- ❖ **The General Inspectorate for Immigration** subordinated to the Ministry of Internal Affairs, as responsible authority in the field of immigration and visas, for the purposes provided for in Articles 24-27 of EES Regulation, as well as Article 14 paragraph (8) of EES Regulation.

Access to the data in the system may be granted, under expressly provided conditions, to the **designated authorities** responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences.

Pursuant to art. 4 of Law no. 300/2022, **the Romanian authorities designated** to request the consultation of the data recorded in the EES Central System are the following:

- ❖ within the Ministry of Internal Affairs: Romanian Police, Romanian Border Police, General Directorate for Internal Protection, General Directorate for Anti-Corruption;
- ❖ Romanian Intelligence Service;
- ❖ Foreign Intelligence Service;
- ❖ within MAPN (the Ministry of National Defense): General Directorate of Defense Intelligence;
- ❖ Protection and Security Service;
- ❖ within the Public Ministry: the Prosecutor's Office attached to the High Court of Cassation and Justice and its subordinate structures and units;
- ❖ Romanian Customs Authority.

The EES provides authorities with information about:

- ❖ Identifying information
- ❖ Biometric data (fingerprints and facial image);
- ❖ Travel document details;
- ❖ Visa data;
- ❖ Travel data;
- ❖ Data on refusal of entry.

Carriers use a dedicated web service to verify that the TCNs they are transporting have already used the number of entries authorized by their visa.

You can access the specially created web service, which allows you, based on information related to the travel document and the expected date of entry or exit, **to check whether or not you are within the authorized duration of stay and, if applicable, the remaining duration of authorized stay.**

1.6. Storage of personal data

Pursuant to Article 34 paragraph (1) of EES Regulation, each entry/exit record or refusal of entry associated with an individual file shall be kept in the EES Central System for a period of **three years** from the date of the exit record or refusal of entry record, as the case may be.

Each individual file together with the associated entry/exit record(s) or refusal of entry record(s) shall be kept in the EES Central System for **a period of three years and one day** from the date of the last exit record or refusal of entry record, if no new entry record is recorded within three years from the date of the last exit record or refusal of entry record.

Pursuant to Article 34 paragraph (3) of EES Regulation, if, after the expiry date of the duration of the authorised stay, no exit record is recorded, the **data are stored for a period of five years**, which starts to run from the day following the expiry date of the duration of the authorised stay. The EES automatically informs Member States three months prior to the scheduled deletion of data on overstayers to enable them to take appropriate action.

1.7. Technical architecture of the Entry/Exit System (EES)

EES is composed of the following items:

- ❖ A central system (the central system of EES);
- ❖ A national uniform interface (National Uniform Interface -NUI) in each Member State, based on common technical specifications and identical for all Member States, which allows the connection of EES Central System to the national border infrastructures in the Member States in a secure manner;
- ❖ A secure communication channel between EES Central System and VIS Central System;
- ❖ A communication infrastructure, which must be secure and encrypted, between EES Central System and NUI;
- ❖ The web service referred to in Article 13 of Regulation (EU) 2017/2226;
- ❖ The centrally established data register, as referred to in Article 62 paragraph (2) of Regulation (EU) 2017/2226.

2. THE RIGHTS OF DATA SUBJECTS WHOSE DATA ARE PROCESSED IN THE ENTRY/EXIT SYSTEM (EES)

Data processing in the Entry/Exit System (EES) is carried out in accordance with European and national data protection rules. The rights of **access**, **rectification/completion**, **erasure** of data subjects and **restriction** of processing of personal data in the EES shall be exercised in accordance with:

- ❖ [Regulation \(EU\) 2017/2226](#) of the European Parliament and of the Council *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, laying down 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.*
- ❖ [Law no. 300/2022](#) *establishing the organizational framework for the national operationalization of the Entry/Exit System and the European Travel Information and Authorization System;*
- ❖ [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council *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 Regulation on data protection);*
- ❖ [Law no. 190/2018](#) *on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council 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/CE (General Data Protection Regulation), as amended;*
- ❖ [Directive \(EU\) 2016/680](#) of the European Parliament and of the Council *on the protection of natural persons regarding the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or executing*

penalties and on the free movement of such data and repeal of the Council's Framework Decision 2008/977/JHA;

- ❖ [Law no. 363/2018](#) regarding the protection of natural persons regarding the processing of personal data by the competent authorities for the purpose of prevention, discovery, investigation, criminal prosecution and combating of crimes or the execution of punishments, educational and safety measures, as well as regarding the free circulation of these data, as the case may be.

According to Regulation (EU) 2017/2226, the rights of data subjects in the context of data processing in the EES are the following:

- ❖ The right to information, according to art. 50
- ❖ The right of access to data, according to art. 52 paragraph (1);
- ❖ The right to rectification/completion of the data, according to art. 52
- ❖ The right to erasure the data, according to art. 52
- ❖ The right to restriction of processing, according to art. 52
- ❖ The right to appeal, according to art. 52.

2.1 The right to information

For the effective application of the provisions on the protection of personal data processed in the EES, the information to be provided to the data subject according to Articles 13 and 14 of GDPR refer to EES Regulation.

Thus, according to **art. 13 of GDPR**, where personal data relating to a data subject are collected from it, the controller, at the time of obtaining such personal data, shall provide the data subject **with all of the following information, unless that person already has that information:**

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the Data Protection Officer, as appropriate;
- the purposes for which the personal data are processed, as well as the legal basis for the processing;
- the recipients or categories of recipients of the personal data;
- additional information, such as: the period for which the personal data will be stored; the existence of the right to request from the controller, with regard to the personal data relating to the data subject, access to, rectification, erasure or restriction of processing; the right to lodge a complaint with a supervisory authority; if the provision of personal data is a legal obligation, as well as if the data subject is obliged to provide such personal data, the existence of automated decision-making, including profiling. Where the controller intends to further process the personal data for a purpose other than that for which they were collected, the controller shall provide the data subject, before such further processing, with information on that secondary purpose and any relevant additional information.

According to **Article 14 of GDPR**, where the personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the Data Protection Officer, as appropriate;
- the purposes for which the personal data are processed, as well as the legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data;
- where applicable, the intention of the controller to transfer the personal data to a recipient in a third country.

This information shall not be transmitted in the following situations:

- the data subject already has the information;
- providing such information proves impossible and requires disproportionate effort;
- **obtaining or disclosure of the data is expressly provided for by Union or national law;**
- where the personal data must remain confidential pursuant to a statutory obligation of professional secrecy governed by Union or national law, including a legal obligation of secrecy.

In addition, according to **art. 50 of EES Regulation**, '*third-country nationals whose data are to be recorded in the EES shall be informed*' of the following:

- that EES can be accessed by Member States and Europol for law enforcement purposes;
- the obligation of visa-exempt third-country nationals, as well as holders of an TFD¹, to allow their fingerprints to be taken;
- the obligation on all third-country nationals who are subject to registration in EES to allow their facial image to be recorded;
- that the collection of data is mandatory for the examination of entry conditions;
- that entry will be refused if a third-country national does not consent to provide the biometric data required for registration, verification or identification in EES;
- the right to receive information in relation to their maximum authorised stay in accordance with Article 11 paragraph (3) of EES Regulation;
- that personal data stored in EES may be transferred to third countries or international organisations listed in Annex I for return purposes², to third countries in accordance with Article 41 (6) of EES Regulation and to Member States in accordance with Article 42 of EES Regulation;
- the existence of the right to request from the controller access to data relating to them, the right to request that inaccurate data relating to them be rectified, that incomplete personal data relating to them be completed, that unlawfully processed personal data concerning them be erased or that the processing thereof be restricted, as well as the right to receive information on the procedures for exercising those rights, including the contact details of the controller and the supervisory authorities or of the European Data Protection Supervisor, if applicable, which shall hear complaints concerning the protection of personal data;
- the fact that EES data will be accessed for border management and facilitation purposes and that overstays will automatically lead to the addition of their data to the list of identified persons referred to in Article 12 paragraph (3), as well as the possible consequences of overstaying;
- the data retention period established for entry and exit records, refusal of entry records and individual files in accordance with Article 34 of EES Regulation;
- the right for overstayers to have their personal data erased from the list of identified persons referred to in Article 12 paragraph (3) and rectified in EES, where they provide evidence that they exceeded the authorised duration of stay due to unforeseeable and serious events;
- the right to lodge a complaint with the supervisory authorities.

¹Transit Facilitating Document;

²UN organizations (such as UNHCR), the International Organization for Migration (IOM), the International Committee of the Red Cross, under the conditions of Article 41 paragraph (2);

2.2. The of access to data

The **right of access to data** is provided for in **art. 52 of EES Regulation**, **art. 15 of GDPR** and **art. 16 of Law no. 363/2018**. The data subject has the right to obtain from the controller a confirmation as to whether or not personal data concerning him or her is being processed and, if so, access to the respective data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or are to be disclosed, in particular recipients from third countries or international organisations;
- the period for which the personal data will be stored or, if this is not possible, the criteria used to establish this period;
- the existence of the right to request from the controller the rectification or erasure of personal data or the restriction of the processing of personal data relating to the data subject or the right to object to the processing;
- the right to lodge a complaint with a supervisory authority;
- if the personal data are not collected from the data subject, any available information on their source.

2.3. The right to rectification, completion and erasure of personal data and to restriction of the processing thereof

2.3.1. The to rectification and completion

According to **art. 52 of EES Regulation**, **art. 16 of GDPR** and **art. 18 paragraph (1) of Law no. 363/2018**, the data subject has the right to obtain from the controller:

- **rectification** of inaccurate personal data concerning him/her;
- **filling in** data that are incomplete, including by providing a supplementary statement, taking into account the purposes for which the data were processed.

2.3.2. The right to erasure (right to be forgotten)

The **right to delete the data and the right to be forgotten**, provided for by **art. 52 of EES Regulation**, **art. 17 of GDPR** and **art. 18 paragraph (3) of Law no. 363/2018**, stipulates that the data subject has the right to obtain from the controller the deletion of personal data concerning him/her, without undue delay, and the controller has the obligation to delete personal data, if one of the following reasons applies:

- personal data are no longer necessary for the purposes for which they were collected or processed;
- personal data has been processed unlawfully;
- personal data must be erased in order to comply with a legal obligation incumbent on the controller under Union law or the national law to which the controller is subject to.

The aforementioned shall not apply to the extent that processing is necessary:

- for complying with a **legal obligation** that provides for processing based on Union law or internal law that applies to the controller or for the performance of a task executed in the public interest or in the exercise of an official authority with which the controller is vested;
- for the establishment, exercise or defense of a right in court.

2.3.3 The right to restriction of processing

The **right to restriction of processing** is regulated by **art. 52 of EES Regulation**, **art. 18 of GDPR** and **art. 18 paragraph (4) of Law No. 363/2018**. The data subject shall have the right to obtain from the controller the restriction of processing where one of the following applies:

- the data subject disputes the accuracy of the data for a period which allows the controller to verify the accuracy of the data;

- the processing is unlawful and the data subject opposes the deletion of personal data, requesting instead the restriction of their use;
- the controller no longer needs the personal data for the purposes of processing, but the data subject requests them for the establishment, exercise or defence of a right in court.

2.3.4. Exceptions (Article 52 of EES Regulation)

If a request for **rectification, completion or erasure** of personal data or **restriction** of processing of such data is addressed to the General Inspectorate of the Border Police and Romania **is not the Member State that entered such data into EES**, the controller shall verify the accuracy of the data and the lawfulness of the processing in EES within **30 days** of its receipt, if such verification can be carried out without consulting the Member State that entered the data into EES, **hereinafter referred to as the responsible Member State**. Otherwise, the GIBP contacts the authorities of the responsible Member State within **7 days** and they verify the accuracy of the data and the lawfulness of the processing in EES within **30 days**.

If the data recorded in EES contains factual errors, is incomplete or has been recorded unlawfully, the responsible Member State or the controller to whom the request has been made **shall rectify, supplement or erase** the personal data or **restrict** their processing in accordance with **Article 35 of EES Regulation**. The responsible Member State or, where applicable, the controller to whom the request has been made shall confirm **in writing** and **without delay** to the data subject that it has taken steps to rectify, supplement or erase the personal data of that person or to restrict the processing of such data.

If the visa data recorded in EES contain factual errors, are incomplete or have been recorded unlawfully, the responsible Member State or, where applicable, the requested controller shall first verify the accuracy of those data in VIS and, if necessary, amend them in EES.

If the data recorded in VIS are identical to those from EES, the responsible Member State or, where applicable, the requested controller shall contact the authorities of the Member State which is responsible for entering those data in VIS within **seven days**. The Member State which is responsible for entering the data in VIS shall verify the accuracy of the visa data concerned and the lawfulness of its processing in the EES within **30 days** of such contact and inform the responsible Member State or the requested controller which, if necessary and without delay, rectifies or supplements the personal data of the data subject or restricts the processing of such data in EES or deletes such data from EES and, where applicable, from the list of identified persons referred to in Article 12 paragraph (3) of EES Regulation.

If the responsible Member State or, where applicable, the requested controller does not agree that the data recorded in EES contain factual errors, are incomplete or have been recorded unlawfully, that Member State shall adopt an administrative decision explaining to the third-country national concerned **in writing** and **without delay** the reasons why the **State is not willing to rectify, supplement, erase personal data concerning him/her nor to restrict the processing of such data**.

The Member State which adopted the administrative decision shall also provide the third-country national concerned with information detailing the measures he or she may take if he or she does not accept the explanation. That information shall include details of how to bring an action or complaint before the competent authorities or courts of that Member State and of any assistance that is available in accordance with laws, regulations and procedures of that Member State, including from the supervisory authority established in accordance with Article 51 paragraph (1) of Regulation (EU) 2016/679.

2.4. The right to appeal

Without prejudice to Articles 77 and 79 of Regulation (EU) 2016/679, any person **shall have the right to bring an action or complaint** before the competent authorities or courts of the Member State which denied him/her the right of access to data or the right to rectification, completion or erasure of such data, as provided for in Articles 52 and 53 paragraph (2) of EES Regulation.

The right to bring such an action or to lodge such a complaint also applies in cases where requests for access, rectification, completion or erasure have not been answered within the time limits set out in Article 52 of EES Regulation or have not been processed at all by the data controller.

2.4.1. The right to lodge a complaint with a supervisory authority (art. 77 of GDPR and art. 20 of Law no. 300/2022)

Without prejudice to any other administrative or judicial remedy, the data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if he or she considers that the processing of personal data relating to him or her infringes legal provisions.

The supervisory authority with which the complaint has been lodged shall inform the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78 of GDPR.

2.4.2. The right to address the court (art. 79 of GDPR)

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77 of GDPR, data subject shall have the right to an effective judicial remedy if he or she considers that his or her rights have been infringed.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

3. PROCEDURE FOR EXERCISING THE DATA SUBJECT RIGHTS

In order to exercise the rights provided for by EES Regulation, you may submit a **written** request, **dated** and **signed**, by mail at the address: **Bucharest, 42 C Geniului Avenue, district 6, postal code 060117**, by fax: 021.312.11.89 or using e-mail address: **pfr@igpf.ro** or **dataprotection.igpf@igpf.ro**.

You can also submit it in person at the public relations counter at the headquarters of the General Inspectorate of the Romanian Border Police or at any data controller within the Ministry of Internal Affairs or its territorial structure, which transmits the GIBP request, within **5 days** from the date of its receipt.

If you make the **request in electronic format**, the information is provided in electronic format where possible, unless you request another format.

Requests must be **drafted, dated and signed by** the person whose data has been processed and are considered valid only if **you prove your identity** (with a copy of an identity document). Requests for rectification, completion and/or deletion must necessarily include the **personal data whose rectification, completion and/or deletion is requested**.

Pursuant to Article 52 paragraph (6) of EES Regulation, **any application shall contain the minimum information necessary to identify the third-country national concerned.** For this purpose, fingerprints may only be requested in duly justified cases and if there are significant doubts about the identity of the applicant. This information is used solely to enable the third-country national to exercise his/her rights and is then immediately deleted.

If it does not take action on the request of the data subject, the GIBP shall inform the data subject, without delay and no later than one month after receipt of the request, of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and of seeking a judicial remedy.

In order to defend the rights provided by EES Regulation, the persons whose personal data are the subject of processing carried out within the General Inspectorate of the Border Police, may submit a complaint to The National Supervisory Authority for Personal Data Processing (NSAPDP) at its headquarters in Bucharest, 28-30 G-ral Gheorghe Magheru Avenue, district 1, postal code 010336, fax: 031.805.96.02, website: <https://www.dataprotection.ro/index.jsp?page=home&lang=en> or using e-mail: anspdc@dataprotection.ro.

To file a complaint with NSAPDP [click here](#).

3.1. Exercise of the rights of the data subject by representation

Pursuant to Article 80 of GDPR, the data subject has the right to mandate a not-for-profit body, organisation or association, which has been properly constituted in accordance with national law, whose statutory objectives are in the public interest, which is active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of their personal data, to lodge the complaint on his/her behalf, to exercise on his/her behalf the rights referred to in Articles 77, 78 and 79 of GDPR, as well as to exercise the right to receive compensation referred to in Article 82 on behalf of the data subject, if provided for in national law.

Member States may provide that any body, organisation or association referred to in Article 80, paragraph (1) of GDPR, independently of the mandate of a data subject, has the right to lodge a complaint in that Member State with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79, if it considers that the rights of a data subject under GDPR have been infringed as a result of the processing.

4. TERMS

Pursuant to Article 52 of EES Regulation, the responsible Member State or the requested Member State is obliged to respond within **45 days** of receipt of the request.

5. RESTRICTIONS AND EXCEPTIONS

5.1. Restrictions

Restrictions on the exercise of the rights of the data subjects are provided for in Article 23 of Regulation (EU) 2016/679 and Article 17 paragraph (1) of Law no. 363/2018. Union or Member State law to which the controller or processor is subject to may restrict, by way of a legislative measure, the scope of the obligations and rights provided for in Articles 5, 12 to 22 and 34 of GDPR, insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 of Regulation (EU) 2016/679, where such restriction respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society to ensure:

- (a) national security;
- (b) the defence;

- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and fiscal matters and matters of public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics in regulated professions;
- (h) the monitoring, inspection or regulatory function related, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- i) protection of the data subject or the rights and freedoms of others
- (j) enforcing civil law claims.

5.2. Exceptions

Exceptions provided for by Law no. 363/2018 are:

- postponement, restriction or omission of the provision of information at the request of the data subject (art. 15)
- Limitations to the right of access to data (art. 17).

Pursuant to Article 20 of Law no. 363/2018, in the situations provided for in art. 15, 17 paragraph (3) and art. 19, paragraph (6) of Law no. 363/2018, the data subject may apply to the supervisory authority for the exercise of the rights provided for by law.

The controller has the obligation to inform the data subject of the possibility provided for in art. 20 paragraph (1) of Law no. 363/2018.

In the situation of art. 20 paragraph (1) of Law no. 363/2018, the supervisory authority shall take the necessary measures in accordance with its legal duties. The supervisory authority informs the data subject about the issues found, as well as about the possibility to address the court.

6. CONTACT DETAILS

The General Inspectorate of the Border Police (GIBP)

headquarters: Bucharest, 42C Geniului Avenue, district 6, postal code 060117

e-mail: pfr@igpf.ro

phone number: 021.316.25.98, 021.318.25.92

fax: 021.312.11.89

information phone: (+4)0219590

The Data Protection Officer

Within GIBP exists the [Personal Data Protection Department](#):

headquarters: Bucharest, 42C Geniului Avenue, district 6, postal code 060117

e-mail: dataprotection.igpf@igpf.ro / sergiu.malita@igpf.ro

phone number: 021.316.25.98 / interior 19.270

fax: 021.316.35.11

The National Supervisory Authority for Personal Data Processing (NSAPDP)

headquarters: Bucharest, 28-30 G-ral Gheorghe Magheru Avenue, district 1, postal code 010336

website: www.dataprotection.ro

e-mail: anspdcpc@dataprotection.ro

phone number: 031.805.92.11

fax: 031.805.96.02

To file a complaint with NSAPDP [click here](#).

7. DEFINITIONS

- **‘personal data’** - any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **‘processing’** - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **‘controller’** - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **‘processor’** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **‘supervisory authority’** - an independent public authority which is established by a Member State pursuant to art. 51 of GDPR;
- **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:
 - the controller or processor is established on the territory of the Member State of that supervisory authority;
 - data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing;
 - or
 - a complaint has been lodged with that supervisory authority;
- **‘personal data breach’** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.
- **‘Immigration Responsible Authority’** – the competent authority responsible, in accordance with national law, for one or more of the following:
 - to verify, on the territory of the Member States, the fulfilment of the conditions of entry or authorised stay on the territory of the Member States;
 - examine the conditions relating to the residence of third-country nationals on the territory of the Member States and take decisions to that effect in so far as that authority does not

constitute a ‘determining authority’ as defined in Article 2 (f) of Directive 2013/32/EU of the European Parliament and of the Council and, where appropriate, to provide advice in accordance with Regulation (EC) no. 377/2004 of the Council;

- the return of third-country nationals to a third country of origin or transit;
- **‘Visa Responsible Authority’** - *the visa authority as defined in Article 4 paragraph (3) of Regulation (EC) no. 767/2008;*
- **‘Third-country national’** - *any person who is not a citizen of the Union within the meaning of Article 20 paragraph (1) of TFEU, with the exception of persons enjoying the right of free movement equivalent to that of Union citizens under agreements between the Union and its Member States, on the one hand, and third countries, on the other.*

Information on the processing of personal data in EES can be found at the link: <https://www.mai.gov.ro/pliante-si-afise-privind-ees-destinate-publicului>.

Further data about EES can be obtained from the European Commission’s website: https://travel-europe.europa.eu/ees_en.

8. TEMPLATE FOR EXERCISING RIGHTS

8.1. Application for exercising the right of access

| | |
|---|--|
| To | MINISTRY OF INTERNAL AFFAIRS GENERAL INSPECTORATE OF THE BORDER POLICE <i>42C Geniului Avenue, district 6, Bucharest</i> |
| <p>The undersigned (<i>last and first name</i>) _____, ID document/Passport no. _____, located at/residing at _____, street _____, no. _____, building____, apartement __, county/district_____, phone no. _____ (<i>optional</i>), e-mail _____(<i>optional</i>), pursuant to Article 52 of Regulation (EU) 2017/2226 of the European Parliament and of the Council <i>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, laying down 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</i>, I request you to let me know if the personal data concerning me have been processed by your institution, during the period/date _____</p> <p>Additional clarifications: _____</p> <p>_____ (<i>optional</i>).</p> <p>The application is submitted through the representative _____ (mention his/her identity data), for which purpose he/she submits the power of attorney/notarial power of attorney for representation (mention the appropriate variant).</p> <p>Pursuant to Article 52 paragraph (6) of Regulation (EU) 2017/2226, in order to verify my identity as a data subject requesting access to his/her personal data, <u>I enclose a copy of the identity document.</u></p> <p>I request that the answer be communicated to me:</p> <p style="margin-left: 40px;">a) at the address _____ (<i>mention the mailing address</i>);</p> <p style="margin-left: 40px;">b) by e-mail, to: _____.</p> <p>In view of the above, please dispose the legal measures to receive the information required under Regulation (EU) 2017/2226.</p> <p>I declare, under my own responsibility that the data filled in this application is true and correct.</p> | |
| DATE | SIGNATURE |

8.2. Application for exercising the right to rectification/completion

To,

MINISTRY OF INTERNAL AFFAIRS
GENERAL INSPECTORATE OF THE BORDER POLICE
42C Geniului Avenue, district 6, Bucharest

The undersigned (*last and first name*) _____, ID document/Passport no. _____, located at/residing at _____, street _____, no. ____, building____, apartement __, county/district_____, phone no. _____ (*optional*), e-mail _____(*optional*), pursuant to **Article 52 of Regulation (EU) 2017/2226** of the European Parliament and of the Council *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, laying down 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*, please dispose the legal measures to **rectify/supplement** (mention the appropriate version) the following personal data concerning me _____

_____ (*list the respective data*), for the following reasons:

_____ (*state the reasons*).

The application is submitted through the representative _____ (*mention his/her identity data*), for which purpose he/she submits the power of attorney/notarial power of attorney for representation (*mention the appropriate variant*).

Pursuant to Article 52 paragraph (6) of Regulation (EU) 2017/2226, in order to verify my identity as a data subject making the request for **rectification/completion** of personal data, **I enclose a copy of the identity document.**

I request that the answer be communicated to me:

- a) at the address _____ (*mention the mailing address*);
- b) by e-mail, to: _____.

In view of the above, please dispose the legal measures to receive the information required under Regulation (EU) 2017/2226.

I declare, under my own responsibility that the data filled in this application is true and correct.

DATE

SIGNATURE

8.3. Request for exercising the right to erasure

To,

MINISTRY OF INTERNAL AFFAIRS
GENERAL INSPECTORATE OF THE BORDER POLICE
42C Geniului Avenue, district 6, Bucharest

The undersigned (*last and first name*) _____, ID document/Passport no. _____, located at/residing at _____, street _____, no. __, building____, apartment __, county/district_____, phone no. _____ (*optional*), e-mail _____(*optional*), pursuant to **Article 52 of Regulation (EU) 2017/2226** of the European Parliament and of the Council *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, laying down 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*, please dispose the legal measures to **delete** the following personal data concerning me (please list the data) _____

_____for the following reasons:

_____(*optional*).

The application is submitted through the representative _____ (mention his/her identity data), for which purpose he/she submits the power of attorney/notarial power of attorney for representation (*mention the appropriate variant*).

Pursuant to Article 52 paragraph (6) of Regulation (EU) 2017/2226, in order to verify my identity as a data subject making the request **for deletion of** personal data, I enclose a copy **of the identity document**.

I request that the answer be communicated to me:

- a) at the address _____ (*mention the mailing address*);
- b) by e-mail, to: _____.

In view of the above, please dispose the legal measures to receive the information required under Regulation (EU) 2017/2226.

I declare, under my own responsibility that the data filled in this application is true and correct.

DATE

SIGNATURE

** The duration of filling in an application for the exercise of rights may vary depending on the additional information that the data subject wishes to mention. The standard application information can be completed in approximately 5 minutes.*