2025

ROMANIA
MINISTRY OF INTERNAL AFFAIRS
GENERAL INSPECTORATE OF THE BORDER POLICE

INFORMATION NOTE REGARDING THE PROCESSING OF PERSONAL DATA BY THE ROMANIAN BORDER POLICE IN VISA INFORMATION SYSTEM (VIS)

This information note explains how the Romanian Border Police collects, uses and protects personal data, in accordance with the provisions of Regulation no. 767/2008 The VIS Regulation) and Law no. 271/2010. You will find details about your rights regarding personal data, the reasons and grounds for their processing, the recipients of the data, as well as the safeguards applied.

Table of contents

1. INFORMATION ON THE PROCESSING OF PERSONAL DATA BY THE ROMANIAN BORDER POLICE BY VISA INFORMATION SYSTEM (VIS)

1.1. Identity of the data controllers within the Romanian Border Police

This notice aims to provide general information about the processing of your personal data and the rights you have under EU Regulation 2016/679 and the national legislation on the protection and security of personal data, in force.

In accordance with the national and European legislation, in force, the General Inspectorate of the Romanian Border Police (GIBP), in its capacity as personal data controller, is constantly concerned with ensuring the protection of individuals with regard to the processing of personal data it carries out according to the legal framework in force.

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, ensuring public order and tranquility in the area of competence, according to the law.

In accordance with **GEO no. 104/2001** provisions *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 the law.

The Romanian Border Police has in its structure the central unit, territorial units and educational units that process personal data. Thus, within the Romanian Border Police there are distinct data controllers: *General Inspectorate of the Romanian Border Police (G.I.B.P.), Territorial Inspectorates of the Border Police (T.I.B.P. Iași, T.I.B.P. Giurgiu, T.I.B.P. Timișoara, T.I.B.P. Oradea and T.I.B.P. Sighetu Marmației) and Constanta Coast Guard.*

1.2. General information about the General Inspectorate of the Romanian Border Police

The General Inspectorate of Border Police (GIBP) is the central unit of the 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 and investigation of particularly serious crimes circumscribed to organized crime, illegal migration and cross-border crime committed in the area of territorial competence of the 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 **EU Regulation 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).*

2. THE LEGAL BASIS FOR THE PROCESSING

- EU Regulation 2016/399 of the European Parliament and the Council *regarding the Union Code on the border crossing regime for persons* (Schengen Borders Code);
- EU Regulation 2017/458 of the European Parliament and of the Council *amending EU Regulation 2016/399 as regards the strengthening of checks against relevant databases at the external borders;*

- The Convention for the Application of the Schengen Agreement of 14 June 1985, signed at Schengen on 19 June 1990, *on the gradual abolition of checks at common borders, as subsequently amended and supplemented;*
- EU Regulation 2019/817 of the European Parliament and of the Council *on establishing a framework for interoperability between EU information systems in the field of borders and visa;*
- EC Regulation 2009/810 of the European Parliament and of the Council *on the establishment of a Community Visa Code;*
- EU Decision 2024/210 of the Council *on the full application of the provisions of the Schengen acquis in the Republic of Bulgaria and Romania;*
- EU Regulation 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 Data Protection Regulation);*
- EU Directive 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;*
- GEO no. 104/2001 *on the organization and functioning of the Romanian Border Police, as subsequently amended and supplemented, republished;*
- GEO no. 105/2001 *on the state border of Romania;*
- GD no. 445/2002 *for the approval of the methodological norms for the application of the O.U.G. no. 105/2001;*
- GEO no. 194/2002 *on the regime of foreigners in Romania;*
- GEO no. 103/2006 *on some measures to facilitate international police cooperation, as subsequently amended and supplemented, republished;*
- GEO no. 102/2005 *on the free movement on the territory of Romania of the citizens of the Member States of the European Union, the European Economic Area and the citizens of the Swiss Confederation;*
- Law no. 190/2018 *on measures to implement EU Regulation 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 Data Protection Regulation)*
- 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 this data*
- Law no. 102/2005 *on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, republished, as subsequently amended and supplemented;*

3. VISA INFORMATION SYSTEM (VIS)

3.1. What is VIS?

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.

3.2. What is the purpose of VIS?

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.

3.3. What kind of data is stored in VIS?

10 fingerprints and a digital photograph are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database.

10-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

At the Schengen Area's external borders, the visa holder's finger scans may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused – it will merely lead to further checks on the traveller's identity.

In accordance with Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 *concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)* data is stored in the VIS database when:

- lodging the application (Article 9)
- added for a visa issued (Article 10);
- added where the examination of the application is discontinued (Article 11);
- added for a visa refusal (Article 12);
- added for a visa annulled or revoked or with a shortened validity period (Article 13);
- added for a visa extended (Article 14).

Data stored into the database concerns the identity of the authority examining the application, elements (like date, type of the visa) on the application process itself, the name of the applicant, the purpose of the travel, the length of the stay, a photography and fingerprintS.

Data is kept in the VIS system for up to 5 years. This retention period starts from the expiry date of the issued visa, the date a negative decision is taken or the date a decision to modify an issued visa is taken.

Data is fed into the VIS by national authorities. The authorities with access to VIS must ensure that its use is limited to that which is necessary, appropriate and proportionate for carrying out their tasks. Furthermore, they must ensure that in using VIS, the visa applicants and holders are not discriminated against and that their human dignity and integrity are respected.

3.4. Which countries use VIS and who operates it?

As a Schengen instrument, VIS applies to all Schengen States. The EU Agency for large-scale IT systems, eu-LISA, is responsible for the operational management of VIS.

3.5. Who can access VIS?

Competent visa authorities may consult the VIS for the purpose of examining applications and decisions related thereto.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories.

Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application.

In specific cases, national authorities and Europol may request access to data entered into the VIS for the purposes of preventing, detecting and investigating terrorist and criminal offences.

3.6. How is my data in VIS protected?

Access to VIS data is limited to authorised staff in the performance of their tasks. They must ensure that the use of VIS data is limited to that which is necessary, appropriate and proportionate for carrying out their tasks.

Data is kept in the VIS for five years. This retention period starts from the expiry date of the issued visa, the date a negative decision is taken or the date a decision to modify an issued visa is taken. Any person has the right to be informed about his/her data in the VIS. Any person may request that inaccurate data about him/her is corrected and unlawfully recorded data is deleted.

Each EU State must require a National Supervisory Authority to monitor the lawfulness of the processing of personal data by that country. The European Data Protection Supervisor will monitor the activities at European level.

4. THE NATIONAL VISA INFORMATION SYSTEM (NVIS)

4.1. What is NVIS?

The National Visa Information System (NVIS) is a highly secure IT system, operational exclusively within the Ministry of Foreign Affairs' secure network. It is fully compatible with the specifications of the central Visa Information System (C.VIS) and is designed for the management and exchange of visa-related data. By connecting to C.VIS, the competent authorities of Schengen Member States can input, update, and consult this data electronically.

NVIS has been configured to allow the competent Romanian authorities to participate in this data exchange and to manage, at national level, visa applications submitted by third-country nationals subject to visa requirements for entry into Romania.

By processing data of visa applicants and local border traffic permit (LBTP) applicants in the associated national database, SNIV functions as a secure and restricted-access electronic component in which personal data is processed and included exclusively for clearly defined and lawful purposes related to the examination of visa and LBTP applications submitted by foreign nationals intending to travel to Romania, as well as for the issuance of these documents.

Law No. 271/2010 (NVIS Law) regulates the types of transactions involving personal data processed in NVIS (see Articles 10–25 of the NVIS Law), in line with the provisions of the VIS Regulation.

NVIS specifications evolve in accordance with the developments of the C.VIS specifications, ensuring the permanent compatibility between the two systems.

The personal data processed through NVIS is used strictly for the purposes for which it has been collected and processed (visa and LBTP management).

Romanian Border Police personnel authorized to retrieve data from SNIV and issue visas process personal data based on the following principles:
a) **Lawfulness, fairness, and transparency** – personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) **Purpose limitation** – personal data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research, or statistical purposes shall not be considered incompatible with the initial purposes;
c) **Data minimization** – personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
d) **Accuracy** – personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
e) **Storage limitation** – personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed;
f) **Integrity and confidentiality** – personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures;
g) **Accountability** – the data controller is responsible for ensuring compliance with the above principles and must be able to demonstrate such compliance.
The personal data processed within SNIV is protected in accordance with the applicable legal provisions, with full alignment to the principles outlined above.

4.2. Data subjects rights

In accordance with the applicable legal framework, each person has the right to:

- access VIS-stored information
- request that inaccurate or incorrect data is corrected
- request the removal of its unlawfully processed data
- submit a complaint to the national data protection authority
- turn to the courts.

Pursuant to Article 44 of Law no. 271/2010, the request regarding the exercise of the data subject's rights in the context of the processing of personal data in the National Visa Information System (SNIV) or the Visa Information System (VIS) shall be addressed to the National Visa Centre, and the response shall be communicated to the applicant as soon as possible, but no later than 60 days from the date of receipt of the request.

The deadline provided for above shall be extended to 90 days if the request concerns data that have been entered by another Member State.

The correspondence address for sending requests for exercising the rights in the context of the processing of personal data in SNIV or VIS:

Ministry of Foreign Affairs of Romania through the Diplomatic Missions/Consular Posts of Romania and the National Visa Centre of Romania
Premises: 31 Aleea Alexandru, 1st district, Bucharest, PO 011822
Tel.: +40 21 431 11 00; +40 21 431 15 62; +40 21 319 21 08; +40 21 319 21 25
Fax: +40 21 319 68 62
Email: dpo@mae.ro

4.3. Right to submit a complaint to the data protection authority

The lawfulness of the processing of personal data in SNIV or VIS on the Romanian territory and the transmission of this data abroad, as well as the subsequent exchange or processing of additional information are monitored and subject to the control of the National Supervisory Authority for Personal Data Processing (NSAPDP).

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

According to the Procedure for handling complaints, adopted by Decision no. 133/2018, when submitting the complaints, it is mandatory to specify in detail the subject matter, the actions taken by the petitioner at the level of the complainant data controller or processor, as the case may be, the information available to support the allegations, as well as to attachment of conclusive evidence.

The contact details of ANSPDCP are:

National Supervisory Authority for Personal Data Processing (NSAPDP).
28-30 G-ral Gheorghe Magheru Boulevard
1st district, Bucharest, PO 011336,
Romania
Tel.: +40 31 805 92 11
Fax: +40 31 805 96 02
E-mail: anspdcp@dataprotection.ro

4.4. Right to bring an action before the court

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective

judicial remedy where he or she considers that their rights have been infringed as a result of the processing of their personal data.

5. RESTRICTIONS

5.1. Restrictions and limitations on the exercise of the rights of data subjects

Restrictions on the exercise of the rights of the data subjects are provided for in Article 23 of Regulation (EU) 2016/679.

Union or Member State law to which the data 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 GDPR, 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) enforcement of civil law claims.

Also, the postponement, restriction, omission or limitation of the provision of information at the request of the data subject are provided for in Articles 15 and 17 of Law no. 363/2018.

- postponement, restriction or omission (art. 15);
- limitations to the right of access floor (art. 17).

Pursuant to Article 20 of Law no. 363/2018, in the situations provided for in art. 15, art. 17 paragraph (3), art. 19 paragraph (6) of Law no. 363/2018, the data subject may address 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 Article 20 paragraph (1) of Law no. 363/2018.

In the situation provided for in art. 20 paragraph (1) from Law no. 363/2018, the supervisory authority undertakes the necessary measures according to its legal powers. The supervisory authority informs the person concerned about the issues found, as well as about the possibility of addressing the court.

6. THE NATIONAL SUPERVISORY AUTHORITY FOR THE PROCESSING OF PERSONAL DATA

According to the law on the establishment, organization and functioning (Law no. 102/2005), the National Supervisory Authority for Personal Data Processing (NSAPDP) is the public authority with legal personality, autonomous and independent from any other authority of the public administration, as well as from any natural or legal person in the private field.

The Authority's main objective is to defend the fundamental rights and freedoms of natural persons, in particular the right to intimate, family and private life in connection with the processing of personal data and the free movement of such data. This right has a complex content, of great importance for the freedom and personality of the citizen, and in our country it is guaranteed by the Constitution (art. 26).

The lawfulness of the processing of personal data falling within the scope of EU Regulation 2016/679 and the legislation transposing EU Directive 2016/680 is monitored and controlled by NSAPDP.

For this purpose, the supervisory authority has the following tasks (art. 57 of GDPR):

- monitors and ensures the application of GDPR;
- promotes actions to raise awareness and understanding among the public of risks, rules, guarantees and rights in terms of processing - special attention is paid to activities that are specifically aimed at children;
- provides advice, in accordance with domestic law, to the national parliament, the government and other institutions and bodies regarding legislative and administrative measures related to the protection of the rights and freedoms of natural persons with regard to processing;
- promotes actions to raise awareness of controllers and the persons empowered by them regarding their obligations under GDPR;
- upon request, provides information to any data subject in relation to the exercise of his/her rights in accordance with the regulation and, if necessary, cooperates with the supervisory authorities in other member states for this purpose;
- handles complaints submitted by a data subject, body, organization or association in accordance with art. 80 of GDPR and investigates to an adequate extent the subject of the complaint and informs the complainant about the progress and result of the investigation, within a reasonable time, in particular if a more thorough investigation or coordination with another supervisory authority is required;
- cooperates, including by exchanging information, with other supervisory authorities and provides mutual assistance to ensure the consistency of the application and compliance with GDPR;
- carries out investigations regarding the application of GDPR, including on the basis of information received from another supervisory authority or from another public authority;
- monitors relevant developments, insofar as they have an impact on the protection of personal data, especially the evolution of information and communication technologies and commercial practices;
- adopts standard contractual clauses mentioned in art. 28 paragraph (8) and art. 46 paragraph (2) letter (d) of GDPR;
- draws up and keeps up to date a list in relation to the requirements regarding the impact assessment on data protection, in accordance with art. 35 paragraph (4) of GDPR;
- provides advice on the processing operations referred to in art. 36 paragraph (2) of GDPR;
- encourages the development of codes of conduct in accordance with art. 40 paragraph (1), gives its opinion on them and approves those that offer sufficient guarantees, in accordance with art. 40 paragraph (5) of GDPR;

- encourages the establishment of certification mechanisms as well as seals and marks in the field of data protection in accordance with art. 42 paragraph (1) and approves the certification criteria in accordance with art. 42 paragraph (5) of GDPR;
- where appropriate, carries out a periodic review of the certifications granted, in accordance with art. 42 paragraph (7) of GDPR;
- elaborates and publishes the accreditation criteria of a code of conduct monitoring body in accordance with art. 41 and of a certification body in accordance with art. 43 of GDPR;
- coordinates the accreditation procedure of a code of conduct monitoring body in accordance with art. 41 and of a certification body in accordance with art. 43 of GDPR;
- authorizes the contractual clauses and provisions mentioned in art. 46 paragraph (3) of GDPR;
- approves the mandatory corporate rules in accordance with art. 47 of GDPR;
- contributes to the activities of the committee;
- keeps up-to-date internal records regarding the violations of GDPR and the measures taken, in particular the warnings issued and the sanctions imposed in accordance with art. 58 paragraph (2) of GDPR;
- performs any other tasks related to the protection of personal data.

NSAPDP facilitates the submission of complaints referred to in art. 57 paragraph (1) (f) of GDPR through measures such as making available a complaint submission form that can be completed including in electronic format, without excluding other means of communication.

The performance of the duties of the supervisory authority shall be free of charge for the data subject. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee, based on administrative costs or refuse to deal with them.

Without prejudice to any other administrative or judicial remedies, any data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State where he/she has his habitual residence, where his place of work is located or where it took place the alleged violation, if it considers that the processing of personal data which it targets violates GDPR.

In order to defend the rights provided for by EU Regulation 2016/679 and/or Law no. 363/2018, the persons whose personal data are subject to processing carried out within GIBP, may submit a complaint to NSAPDP at its headquarters in 28-30 G-ral Gheorghe Magheru Avenue, district 1, Bucharest, postal code: 010336, by mail, fax: 031.805.96.02, on website: **www.dataprotection.ro** or using e-mail: anspdcp@dataprotection.ro.

To file a complaint with NSAPDP click here.

During all personal data processing, GIBP is subject to the control of the National Supervisory Authority for Personal Data Processing (https://www.dataprotection.ro/) and develops collaboration relations with the Office of the Personal Data Protection Officer within the Ministry of Internal Affairs, which is the specialized structure that exercises the guidance, coordination and monitoring of the unitary application of the legislation in the field of the protection of individuals with regard to the processing of personal data by the structures and units of the Ministry of Internal Affairs.

The guidelines, decisions and recommendations issued by the National Supervisory Authority for Personal Data Processing, as well as the coordination documents developed by the Office of the Personal Data Protection Officer within the Ministry of Internal Affairs are taken into consideration:

- Law no. 102/2005 *on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, republished, as subsequently amended and supplemented*;
- Law no. 129/2018 *amending and supplementing Law no. 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data*

Processing, as well as for the repeal of Law no. 677/2001 for the protection of individuals regarding the processing of personal data and the free movement of such data;

- NSAPDP decision no. 128/2018 *on the approval of the standard form of the personal data breach notification in accordance with EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*;
- NSAPDP decision no. 133/2018 *on the approval of the Procedure for receiving and resolving complaints*;
- NSAPDP decision no. 161/2018 *on the approval of the Procedure for conducting investigations*;
- NSAPDP decision no. 238/2019 *amending Annex no. 2 to the Procedure for conducting investigations*;
- NSAPDP decision no. 174/2018 *on the list of operations for which it is mandatory to carry out the impact assessment on the protection of personal data*.

Useful Links:

- https://www.dataprotection.ro/
- https://www.edpb.europa.eu/edpb_ro
- https://www.edps.europa.eu/_en
- https://commission.europa.eu/law/law-topic/data-protection_ro
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

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;
‘***filing system of personal data’*** - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

8. PRINCIPLES AND LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

8.1. Principles relating to personal data processing

Pursuant to Article 5 of the General Data Protection Regulation, the personal data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

8.2. Lawfulness of Processing

Pursuant to Article 6 of the General Data Protection Regulation, the processing is lawful only if and to the extent that at least one of the following conditions applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

9. 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 Oficer
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: anspdcp@dataprotection.ro
phone number: 031.805.92.11
fax: 031.805.96.02
To file a complaint with NSAPDP click here.

The Teritorial Inspectorate of the Border Police from SIGHETU MARMAȚIEI
headquarters: Sighetu Marmației, 38 Dragoș Vodă Street, postal code 435500, Maramureș County
e-mail: itpf.sighetu.marmariei@mai.gov.ro;
phone number: 0262 314 528;
fax: 0262 316 446.

The Teritorial Inspectorate of the Border Police from ORADEA
headquarters: Oradea, 2 Calea Aradului Street, postal code 410223, Bihor County
e-mail: ijpf.bihor@mai.gov.ro
phone number: 0259 401 400
fax: 0259 418 924

The Teritorial Inspectorate of the Border Police from TIMIȘOARA
headquarters: Timișoara, 49 Sever Bocu Street, postal code 300278, Timiș County
e-mail: itpf.timisoara@mai.gov.ro
phone number: 0257 306 340
fax: 0256 306 355

The Teritorial Inspectorate of the Border Police from GIURGIU
headquarters: Giurgiu, 36 Mircea cel Bătrân Street, postal code 080036, Giurgiu County
e-mail: itpf.giurgiu@mai.gov.ro
phone number: 0246 213 640
fax: 0246 211 785

The Teritorial Inspectorate of the Border Police from IAȘI
headquarters: Iași, 3-5 George Coșbuc Street, postal code 700469, Iași County
e-mail: itpf.iasi@mai.gov.ro
phone number: 0232 272 220
fax: 0232 460 094

The Coast Guard from CONSTANȚA
headquarters: Constanța, 3 Zmeurei Alley, postal code 900433, Constanța County
e-mail: gardadecoasta.igpf@mai.gov.ro
phone number: 0241 641 188
fax: 0241 698 668

Ministry of Foreign Affairs of Romania through the Diplomatic Missions/Consular Posts of Romania and the National Visa Centre of Romania
Premises: 31 Aleea Alexandru, 1st district, Bucharest, PO 011822
Tel.: +40 21 431 11 00; +40 21 431 15 62; +40 21 319 21 08; +40 21 319 21 25
Fax: +40 21 319 68 62
Email: dpo@mae.ro

Pursuant to Article 44 of Law no. 271/2010, the request regarding the exercise of the data subject's rights in the context of the processing of personal data in the National Visa Information System (SNIV) or the Visa Information System (VIS) shall be addressed to the National Visa Centre, and the response shall be communicated to the applicant as soon as possible, but no later than 60 days from the date of receipt of the request.

This section was updated on 16.07.2025.