PROCESSING OF PERSONAL DATA BY
NATIONAL PASSENGER INFORMATION UNIT
FROM THE GENERAL INSPECTORATE OF THE ROMANIAN BORDER POLICE

The National Passenger Information Unit applies the provisions of the relevant EU and national legislation, ensuring that the rights of individuals with regard to the protection of personal data are permanently respected.

1. IDENTITY OF THE DATA CONTROLLER

The National Passenger Information Unit is a specialized structure, without judicial personality, within the General Inspectorate of the Romanian Border Police, which processes personal data for the purpose of fulfilling its duties, provided by Law no. 284 of 26 November 2018 *on the use of air passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, as well as for the prevention and removal of threats to national security.*

Data controller designation

Pursuant to Article 32 of Law no. 284/2018 within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* and of the legislation implementing it, the General Inspectorate of the Romanian Border Police shall be designated as the data controller for the processing carried out within the PNR Data Filing System. Requests made in the exercise of the rights of data subjects are addressed only to NPIU.

1.1. Contact details

- **CONTACT DETAILS OF NPIU**

Headquarters: Bucharest, 42C Geniului Avenue, district 6, postal code 060117;
E-mail address: unip@igpf.ro
Phone: 021.316.25.98; 021.318.25.92
Fax: 021.312.11.89
Information phone: (+4)0219590.

- **CONTACT DETAILS OF THE NPIU DATA PROTECTION OFFICER**

The NPIU Department for Data Protection of NPIU operates at the level of GIBP
Headquarters: Bucharest, 42C Geniului Avenue, district 6, postal code 060117;
NPIU Data Protection Officers: chief commissioner Dumitru Alexandru-Gabriel and commissioner Popa Cristian-Eduard;
E-mail address: protectiadatelor.unip@igpf.ro
Phone: 021.316.25.98/ 19.270, fax 021.316.35.11.

1.2 Legal basis

European legislation

- Regulation (EU) (2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;
- Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector;
- Convention implementing the Schengen Agreement - art.102-118 - protection of personal data in S.I.S. and art. Personal Data Protection
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, updated;

National legislation

- Law no. 284/2018 on the use of air passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, as well as for the prevention and removal of threats to national security
- Ordinance 34/2006 on the obligation of air carriers to communicate passenger data
- Law no. 363/2018 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of preventing, discovering, investigating, prosecuting and combating criminal offences or the execution of criminal penalties, educational and security measures, as well as on the free movement of such data;
- Law no. 682/2001 on the ratification by Romania of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, updated;
- Law no. 129/2018 amending and supplementing Law nr.102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, as well as repealing Law no. on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector
- Law no. 190/2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council as of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) published in the Official Gazette of Romania no.
- Law no. 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing.

2. NPIU CARRIES OUT THE FOLLOWING MAIN TASKS:

- the collection of PNR data from air carriers, the storage and processing of such data and the transfer of those data or the result of their processing to the competent authorities, under the conditions laid down in Article 20 of Law no. 284/2018;
- the exchange of PNR data and the exchange of the results of the processing of PNR data with the Passenger Information Units of other Member States of the European Union and with EUROPOL, under the conditions laid down in Article 24, 26 and 27 of Law no. 284/2018;
- the exchange of PNR data with third countries, under the conditions set out in Article 28 of Law no. 284/2018.

According to the legal provisions in force, the National Passenger Information Unit has the obligation to respect the privacy and security of the processing of personal data of each person. It also has the obligation to safely administer the data collected for the performance of its legal duties and to ensure the data subjects the rights specifically provided for in Law no. 363/2018, respectively Regulation (EU) 2016/679 (GDPR).

3. WHAT IS MEANT BY PERSONAL DATA?

Personal data means *any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a number, an identification number, location data, an online identifier, or to one or several specific elements, its own physical, physiological, genetic, psychological, economic, cultural or social identities.*

4. PERSONAL DATA PROCESSING

The National Passenger Information Unit processes personal data by using the data from the air passenger name record for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, as well as for the prevention and removal of threats to national security, without the consent of the data subject, for the purpose of fulfilling his/her job duties, in accordance with the law.

Passenger Name Record or PNR - record of each passenger's travel requirements, containing the information necessary to enable the processing and control of bookings by the booking air carriers and participating air carriers, for each journey booked by or on behalf of to any person, regardless of whether it is contained in reservation systems, in departure control systems used to check passengers when boarding an aircraft or in equivalent systems that provide the same functionality.

4.1. Purposes for which pnr data is processed

PNR data contained in the PNR Data Recording System shall only be used for the following purposes:

a) prevention, detection, investigation and prosecution of terrorist offences or serious crime;
b) the prevention and removal of threats to national security provided for in Article 3 of the Law no. 51/1991, republished, as subsequently amended and supplemented.

4.2. PNR data processing by NPIU

NPIU processes the data contained in the PNR Data Filing System exclusively for the following purposes:

a) carrying out an assessment of the passengers before their scheduled arrival or departure in/from Romania, in order to identify the persons in respect of whom further examination by the competent authorities and, as the case may be, by EUROPOL is required, given that those persons may be involved in the commission of a terrorist offence, a serious crime or an activity that constitutes a threat to national security;

b) providing answers, on a case-by-case basis, to a duly justified request based on sufficient grounds from the competent authorities for the provision and processing of PNR data, in specific cases, for the purposes provided for in Article 18 and communicating the results of this processing to the competent authorities or, as the case may be, EUROPOL;

c) analysis of PNR data in order to update or define new criteria to be used for assessments carried out under paragraph (2) (b) in order to identify any persons who may be involved in the commission of a terrorist offence, a serious crime or an activity that constitutes a threat to national security.

4.3. Recipients of the personal data

PNR data or the result of the processing of PNR data may only be communicated to the authorities competent to request or receive these data, provided for in Article 11 of Law no. 284/2018.

4.4. Categories of recipients of personal data:

- the data subject/the data subject's legal representatives;
- competent authorities referred to in Article 11 of Law no. 284/2018;
- Passenger Information Units of other Member States of the European Union and with EUROPOL
- public law enforcement authorities (courts, prosecutors' offices etc.).

4.5. Transfer of data to third countries

NPIU may transfer PNR data or the result of the processing of PNR data to the authorities of a third country only on a case-by-case basis and if the conditions provided for in Article 28 of Law no. 284/2018, after the recipients notify in writing that they intend to use the PNR data in accordance with the conditions and guarantees provided by law.

4.6. Period of data retention

PNR data provided by air carriers shall be kept within the PNR Data Filing System for a period of 5 years from the time of completion of the active transmission of such PNR data from the air carrier systems into the PNR Data Filing System, hereinafter referred to as the time of provision.
At the end of 6 months from the moment of providing PNR data by air carriers, they are depersonalized by masking the following data elements:
a) names, including the names of other passengers on the PNR and number of passengers on the PNR travelling together;
b) the address and contact information associated with the reservation;
c) all information on the form of payment, including the billing address;
d) information from the "loyal customer" profile;
e) the general mentions provided for in Article 14 paragraph (1) section l);
f) any API data that has been collected;
At the end of the 5-year period, the PNR data in the PNR data filing system shall be automatically deleted by an irreversible procedure.

4.7. Categories of processed data

Air carriers shall transmit to NPIU, under the conditions provided for in Article 15 of Law no. 284/2018, the following data from the passenger name record:
a) the booking code;
b) date of reservation/issue of ticket;
c) the scheduled travel date (s);
d) the name and surname associated with the reservation;
e) address and contact information - phone number, email address - associated with the reservation;
f) all information on the form of payment, including the billing address;
g) the complete travel itinerary;
h) information from the "loyal customer" profile;
i) the travel agency or agent through which the reservation was made or the ticket was purchased;
j) travel status of passenger, including confirmations, check-in status, no show or go show information;
k) the split or split information in the passenger name record;
l) general mentions, including all available information about unaccompanied minors under the age of 18, such as the name and gender of the minor, age, spoken language (s), name and contact details of the person accompanying him/her at departure and his/her relationship with the minor, name and contact details of the person waiting for him/her at arrival and his/her relationship with the minor, the agent present at departure and at arrival;
j)ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields;

k) seat number and other seat information;
o) information on shared codes;
p) all baggage information;
q) number and other names of travellers on PNR;
r) any API data collected, including the type, number, country of issue and expiry date of any identity document, nationality, surname, first name, gender, date of birth, airline, flight number, departure date, arrival date, departure airport, arrival airport, departure time and arrival time;
s) a history of all changes to the PNR data referred to in letters a)-r).

5.RIGHTS OF THE DATA SUBJECT

As a guarantee of the achievement of the declared purpose of Law no. 363/2018 and EU Regulation 2016/679, the rights of the data subject are:

- Right to information (Art. 12-14 of Law no. 363/2018 and Art. 13 -14, of the GDPR);
- Right of access for the data subject (Art. 16 of Law no. 363/2018 and Art. 15 of the GDPR);
- Right to erasure (*right to be forgotten*) (Art. 18 of Law no. 363/2018 and Art. 17 of the GDPR);
- The right to complain to a supervisory authority (Art. 57 of Law no. 363/2018 and Art. 77 of the GDPR);
- The right to go to court (Art. 58 of Law no. 363/2018 and Article 79 of the GDPR).

The rights contained in Law no. 363/2018 are rendered below:

5.1. Right to be informed *(art.12 ,13,14 of Law no. 363/2018)*

ART. 12

(1) The controllers are obliged to establish the organizational, technical and procedural measures to provide the data subject with the necessary information according to the provisions of Article 13 and Art. 16-21 and to ensure the transmission of a response in connection with the processing carried out under the conditions provided for in Article 11 or in connection with the notification of data subjects in the event of a security incident, under the provisions of Article 39;
(2) The answer must be formulated in a concise, intelligible and easily accessible form, using clear and simple language.
(3) The information shall be communicated under the conditions set out in paragraph (2) in the same format as the request, with the following exceptions:
a) the identity of the applicant cannot be established accurately, under the conditions provided for in paragraph 10;
b) the format chosen for submitting the request involves risks of unauthorized or unlawful processing or accidental loss, destruction or damage, in relation to the amount of personal data, the degree of sensitivity of the information, especially in the case of the categories of data provided for in Article 10 and the data relating to minors.
(4) The controller is obliged to establish organizational and procedural measures in order to facilitate the exercise of the rights of the data subject under the provisions of Article 11 and Art. 16-21;
(5) The controller has the obligation to inform the data subject, in writing, on how to solve the requests made under this law. The answer shall be sent free of charge, within a maximum of 60 calendar days.
(6) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the data controller may:
a) charge a reasonable fee that takes into account the administrative costs of transmitting or communicating the information or taking the requested measures; or
b) refuse to comply with the request.
(7) The amount of the fee provided for in paragraph (6) (a) shall be established, respectively updated by an administrative act issued at the level of the operator.

(8) The unfounded or excessive nature of the request shall be determined on a case-by-case basis, according to the following criteria:
a) the subject of the request;
b) the repetitive nature of the request;
c) the existence of additional processing of personal data, in relation to those carried out at the time of the previous request.
(9) The unfounded or excessive character of the request, under the conditions set out in paragraph (6), must be demonstrated by the data controller.
(10) If the identity of the person making a request under the provisions of Article 16 or 18 could not be established accurately, the operator asks her for additional information necessary to confirm her identity.
(11) Additional information collected under paragraph (10) may not be processed for any purpose other than to confirm identity and shall be destroyed within 3 years of collection. The data controller may set shorter retention periods.

ART. 13
Data controllers are required to put in place organizational, technical and procedural measures in order to make available to interested persons the following categories of information:
a) the identity and contact details of the data controller;
b) the contact details of the Data Protection Officer, as appropriate;
c) the purposes of the processing for which the personal data are intended;
d) the right to lodge a complaint with the supervisory authority and its contact details;
e) the right to request from the operator access to personal data relating to the data subject or the rectification or erasure of such data or the restriction of their processing.

ART. 14
Upon request, when the law does not provide otherwise, the operator shall communicate to the data subject the information provided for in Article 13, as well as the following additional information:
a) legal basis for the processing;
b) the period for which the personal data are stored or, if this is not possible, the criteria used to determine that period;
c) if applicable, the categories of recipients of personal data, including from third countries or international organizations;
d) any other additional information, depending on the specifics of the processing activities, in particular when the personal data are collected without the knowledge of the data subject.

5.2. The right to acces the data *(art. 16 of Law no. 363/2018)*
ART. 16
(1) The data subject shall have the right to obtain from the controller, upon request and free of charge, confirmation as to whether or not personal data concerning him or her are processed by him or her.
(2) The controllerr is obliged, if it processes personal data concerning the data subject, to communicate it, within a maximum of 60 calendar days from the registration of the request, under the conditions provided for in Article 12 paragraphs (2) and (3), in addition to the confirmation, including the personal data undergoing processing, as well as the following information:
a) the purposes and legal basis of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organizations;
d) the period for which the personal data will be stored or, if this is not possible, the criteria used to establish this period;

e) the right to request from the operator the rectification or erasure of personal data or restriction of processing of personal data relating to the data subject;
f) the right to lodge a complaint with the supervisory authority and its contact details;
communication of the personal data undergoing processing and of any available information as to their source.

5.3. Right to data erasure „right to be forgotten” *(art. 18 of Law no. 363/2018)*
ART. 18
(3) The controller has the obligation to delete, by irreversible procedures, ex officio or at the request of the data subject, the personal data whose processing does not comply with the provisions of Article 1 Para. (2), Art. 5 or 10 times to be deleted by virtue of fulfilling an obligation expressly provided by law.
(4) The controller has the obligation to restrict the processing of personal data, and not to delete them, if one of the following situations occurs:
a) the accuracy of the personal data is contested by the data subject and the accuracy or inaccuracy of those data cannot be established with certainty;
b) personal data must be kept as evidence.
(5) The controller is obliged to communicate to the data subject, under the conditions of Article 12 para. (2)-(4), within a maximum of 60 calendar days from the registration of the request, the confirmation or, as the case may be, the invalidation of the settlement of the requests formulated according to the provisions of para. (1), (2) or (3), the reasons on which the invalidation measure is based, as well as the fact that it may lodge a complaint with the supervisory authority or appeal to the court the decision of the operator.
(6) The time limit provided for in paragraph (5) may be extended by up to 60 calendar days, insofar as the settlement of applications requires complex procedures, in particular the consultation of competent authorities abroad. The data subject shall be informed of the extension of the deadline before the expiry of the initial deadline.
(7) The lifting of the restriction of processing established according to the provisions of paragraph (4) letter a) shall be carried out by the operator, at the same time as the data subject is notified of the measure adopted.
(8) The provisions of paragraph (5) shall not apply if, taking into account the fundamental rights and legitimate interests of the natural person, such a measure is necessary and proportionate in a democratic society to:
a) avoid obstructing the proper conduct of the criminal proceedings;
b) not to prejudice the prevention, discovery, investigation, prosecution and combating of crimes or the execution of penalties;
c) to protect public order and safety;
d) protect national security;
e) protect the rights and freedoms of others.

5.4. The right to file a complaint with a supervisory authority *(art. 57 of Law no. 363/2018)*
ART. 57
(1) If the data subject considers that the processing of personal data concerning him/her violates the provisions of this law, he/she has the right to complain to the supervisory authority.
(2) The provisions of the General Data Protection Regulation shall apply accordingly.

5.5. The right to go to court *(art. 58 of Law no. 363/2018)*
ART. 58
Without prejudice to the possibility of complaining to the supervisory authority, data subjects have the right to appeal to the court to defend any rights guaranteed by this law that have been violated.

6. MODEL OF EXERCISING THE RIGHTS

In order to exercise the rights relating to the processing of personal data carried out by NPIU, an application may be submitted to the headquarters of the General Inspectorate of the Romanian Border Police in Bucharest, 42C Geniului Avenue, district 6, postal code 060117 or can be sent electronically to: unip@igpf.ro

At the level of the General Inspectorate of the Romanian Border Police there is the NPIU Data Protection Compartment, which also has the task of solving the requests of the data subjects.

6.1. Exercise of the rights of the data subject in the context of the processing of personal data within the PNR Data Filing System

ART. 32 of Law 284/2018

(1) The rights of the data subject in the context of the processing of personal data within the PNR Data Filing System shall be exercised in accordance with the General Data Protection Regulation and its implementing legislation, applying the provisions of paragraphs (2) to (6), as well as Article 24 of Law no. 238/2009, republished.

(2) Requests made in the exercise of the rights of data subjects are addressed only to NPIU. A request is valid only if the data subject proves his/her identity under the law.

(3) In order to communicate to the applicant information regarding the personal data processed within the PNR Data Filing System, in the case of the processing provided for in Article 24-29, UNIP requires, as the case may be, the consent of the competent authorities to which the data were transferred, the consent of EUROPOL or the consent of the similar foreign entity that provided the data.

4. The competent authorities shall communicate the option within 20 days from the date of receipt of the request from NPIU.

(5) If the similar entity consulted abroad in accordance with paragraph (3) does not communicate a response in view of the deadlines for responding to the requests of the data subjects, NPIU shall respond to the applicant without indicating the origin of the data.

The personal data controller is obliged to communicate to the data subject information on the actions taken following a request submitted pursuant to Articles 16 and 18 of Law 363/2018, respectively art. 15-22 of the RGPD, without undue delay and within the time limits provided by these normative acts, namely:

- within 60 calendar days – according to Law no. 363/2018;
- within one month of receipt of the request (this period may be extended by two months when necessary, taking into account the complexity and number of requests; the operator shall inform the data subject of any such extension, within one month of receipt of the request, also giving the reasons for the delay) – according to the GDPR.

If it does not take action on the request of the data subject, the data operator 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 seeking a judicial remedy (in accordance with the GDPR).

Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

Any communication and any measures taken pursuant to Articles 13, 16 and 18 of Law no. 363/2018, respectively 15-22 and 34 are provided free of charge.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the operator may:

- charge a reasonable fee taking into account the administrative costs for providing the information or communication or for taking the requested measures or to refuse to comply with the request.

If it has reasonable doubts about the identity of the natural person submitting the request, the operator may request the provision of additional information to the data subject (legitimation - when the request is submitted personally or transmission of a copy of the identity document – when the request is transmitted by post or electronically).

Verification of the identity of the applicant is necessary for the purpose of:

- obtaining reasonable proof of the identity of the applicant/obtaining certain proof of the relationship between the applicant and the data subject, where the request is made on behalf of the data subject;
- protecting personal data against unauthorized or illegal access;
- ensuring the data subject that the operator takes all technical and organizational measures to ensure the security and confidentiality of personal data.

Additional information collected may not be processed for any purpose other than to confirm identity and is destroyed within 3 years of collection. The operator may set shorter retention periods.

6.2. Exceptions to the exercise of rights

The exceptions regarding the exercise of the rights are provided by Law no. 363/2018, as well as the GDPR.

Exceptions provided 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 (Art. 17).

6.3. The measure of postponing, restricting or omitting to provide information to the person

ART. 15

(1) The controller may order, as the case may be, the measure of postponing, restricting or omitting the provision of information to the data subject under the conditions provided for in Article 14 only if, taking into account the fundamental rights and legitimate interests of the data subject, such a measure is necessary and proportionate in a democratic society to:

a) avoid obstructing the proper conduct of the criminal proceedings;

b) avoiding prejudice to the prevention, discovery, investigation, prosecution and combating of crimes or the execution of penalties;

c) protection of public order and safety;

d) protecting national security;

e) protecting the rights and freedoms of others.

(2) The measure of postponing the provision of information shall be ordered for a period that may not exceed one year, if the incidence of conditions that make communication impossible is limited in time. The deferral measure may be extended within the period of one year. Upon the expiry of the term for which the measure of delaying the provision of information was ordered, the operator shall submit the information provided for by law.

(3) The data subject shall be informed in writing, no later than 60 calendar days after the request has been registered, of the extent of the deferral of the provision of information and the reason for its disposition, of the period for which this measure has been ordered, as well as of the fact that he or she may lodge a complaint with the supervisory authority against the decision of the operator or appeal to the court against the decision of the controller.

(4) The measure of restricting the provision of information is ordered if the incidence of conditions that make communication impossible is not limited in time. If the provision of information is restricted, the operator shall send a reply to the data subject. The form and content of the response are determined by each controller.
(5) The measure of failure to provide information shall be ordered if even the mere information of the data subject on one or more processing operations is likely to affect one of the activities referred to in paragraph (1) (a) to (d).
(6) The omission to provide information may be partial or total. In the event of partial omission, the data subject shall be informed, within 60 calendar days of the registration of the request, of the categories of processing that are not likely to affect the activities referred to in paragraph (1). In the event of total omission, the operator shall send a response to the data subject. The form and content of the response are determined by each controller.
(7) The controller is obliged to keep records of the situations in which the measure of omitting to provide information was ordered and to document the adoption of this measure.
(8) In January of each year, the operator has the obligation to inform the supervisory authority on the statistical situation of the omission measures to provide information adopted in the previous year, broken down for each of the activities provided in para. (1) letters a)- d).

6.4. Limitations to the right of access

ART. 17
(1) Provisions of art. 16 shall not apply if, taking into account the fundamental rights and legitimate interests of the natural person, such a measure is necessary and proportionate in a democratic society to:
a) avoid obstructing the proper conduct of the criminal proceedings;
b) avoiding prejudice to the prevention, discovery, investigation, prosecution and combating of crimes or the execution of penalties;
c) protection of public order and safety;
d) protecting national security;
e) protecting the rights and freedoms of others.
(2) The restriction of the right of access may be total or partial and shall be ordered in respect of one or more processing operations where disclosure is likely to affect one of the activities referred to in paragraph (1).
(3) In the situation referred to in paragraph (2), the data subject may be informed of the categories of processing that are not likely to affect the activities referred to in paragraph (1), the reason for adopting this measure, as well as of the possibility of lodging a complaint with the supervisory authority or of addressing the court.
(4) By way of exception to the provisions of paragraph (3), the reason for adopting the measure to limit the right of access shall not be communicated if its disclosure is likely to affect one of the activities referred to in paragraph (1) (a) - (d).
(5) The operator is obliged to keep records of the cases in which the measure limiting the right of access has been ordered and to document the adoption of this measure.
(6) In January of each year, the operator has the obligation to inform the supervisory authority on the statistical situation of the cases in which the measure limiting the right of access was adopted in the previous year, broken down for each of the activities referred to in paragraph (1).

7. The National Supervisory Authority for Personal Data Processing

According to Law no. 102/2005, the National Supervisory Authority for Personal Data Processing (A.N.S.P.D.C.P.) has as its main objective the protection of 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. The legality of the processing of personal data falling under the Regulation and Law no. 363/2018 is monitored and controlled by the Supervisory Authority.

The contact coordinates of A.N.S.P.D.C.P. **are:**
Headquarters in Bucharest, 28-30 G-ral Gheorghe Magheru Avenue, district 1, postal code 010336; Phone: 031.805.92.11, 031.805.92.12; Fax: 031.805.96.02;
Internet: www.dataprotection.ro;
Email: anspdcp@dataprotection.ro;
To file a complaint with NSAPDP click here.

EXERCISE OF THE DATA SUBJECT'S RIGHTS THROUGH REPRESENTATION
Art. 80 of the RGPD
(1) The data subject has the right to mandate a body, organization or not-for-profit association, which has been properly established 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, as well as to exercise the right to receive compensation referred to in Article 82 on behalf of the data subject, if provided for by national law.
(2) Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, 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 this Regulation have been infringed as a result of the processing.

ART. 59 of Law 363/2018
In order to defend his/her rights, the data subject has the right to mandate a body, organization or association, which is not for profit, established under the law, whose statutory objectives are in the public interest and which is active in the field of protection of the rights and freedoms of data subjects with regard to the protection of personal data, to lodge the complaint on his/her behalf and to exercise on his/her behalf the rights provided by this law.

This section was updated on 16.12.2024.