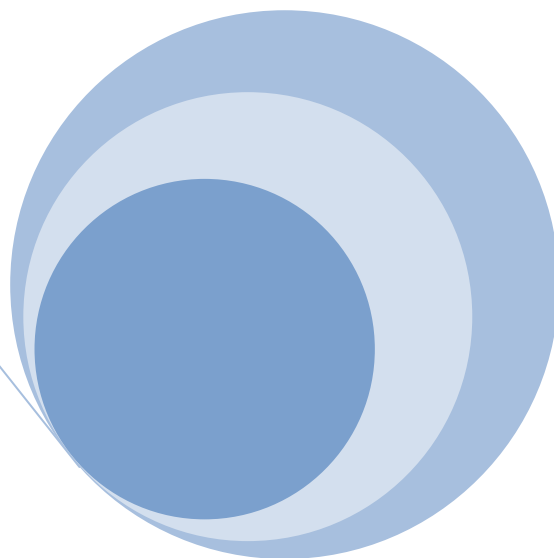
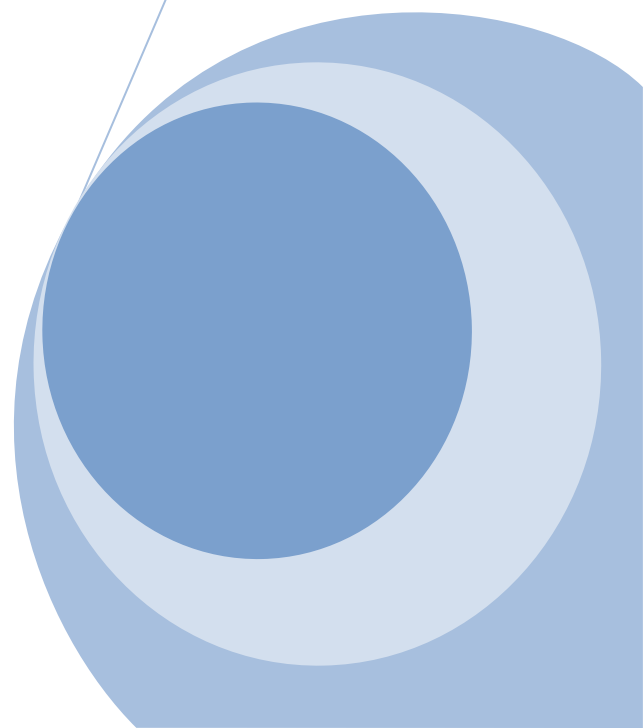


Ministry of Administration and Interior



# Data protection in SIS

---



## CONTENT

Relevant acquis .....	4
Internal Legal Framework.....	5
Implementing the communitarian acquis at national level .....	5
What does the Schengen Information System mean?.....	6
General rules regarding data entered in SIS .....	6
Personal data entered in SIS .....	7
Elements of personal data entered in SIS .....	8
The consent of the person whose personal data is processed .....	9
National authorities competent in managing and exploiting NISA .....	10
Security measures for the protection of personal data .....	11
The rights of the data subject in the context of personal data processing.....	12
Exemption.....	13
Submitting the petition/printed form by a data subject regarding his data protection rights .....	14
Solving the petition submitted by a data subject .....	14
Informing the data subject about other rights .....	15
Complaints addressed to the national supervisory authority for personal data processing .....	16
General information about Schengen area.....	17

The concept of **personal data protection** represents the right of natural person to have those characteristics which may lead to her identification defended and the correlative obligation of the state to adopt adequate measures to ensure an efficient protection.

Personal data represents that information which may be related directly or indirectly to a natural, identified/identifiable person, such as: surname, name, personal numerical code, address, telephone number, facial image, etc

Taking into account the necessity to defend and observe the fundamental right to intimate and private life, personal data protection represents a very important field substantiated by the presence of a distinct chapter in the Schengen Convention.

## RELEVANT ACQUIS

The objective of the provisions of the Communitarian acquis regarding the processing of personal data, taken into account at their transposed into the national legislation, is represented by the **ensuring and protecting the rights and fundamental freedoms of natural persons especially the right of intimate, family and private life.**

The right of intimate and private life is guaranteed by

- 🌀 The Treaty on European Union, art. 6
- 🌀 Charter of Fundamental Rights of the European Union, 7th of December 2000
- 🌀 European Convention of Human Rights, art. 8

### A. 1<sup>st</sup> Pillar

- *Convention* implementing the *Schengen* Agreement – art. 126–130 – personal data protection;
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108 (Strasbourg 29.01.1981);
- Additional Protocol of the Convention regarding Supervisory Authorities and Transborder Data Flows (4<sup>th</sup> of October 2001);
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;

### B. 3<sup>rd</sup> Pillar

- *Convention* implementing the *Schengen* Agreement – art. 102–118<sup>1</sup> – personal data protection in SIS;
- *Recommendation no. R (87) 15 of the committee of ministers to member states* regulating the use of personal data in the police sector;

## ATTENTION!!

**The Schengen Acquis in the field does not aim at secret data/information or classified documents.**

---

<sup>1</sup> Amended by: Council Regulation 2004/871 and by Council Decision 2005/211

- art. 102a was introduced by Regulation (EC) No 1160/2005 of the European Parliament and of the Council replaced by Regulation (EC) No 1986/2006 of the European Parliament and of the Council
- art. 102 – 118 were replaced by the Regulation (EC) No 1987/2006 of the European Parliament and of the Council and by Council decision No. 533/2007( for member states participating at SIS 1+)

## INTERNAL LEGAL FRAMEWORK

Implementing the communitarian acquis at national level

### *Personal data protection – Art. 126 – 139 CAAS*

- The Constitution of Romania, art. 26
- Law no. 682/2001 regarding the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108 (Strasbourg 29.01.1981);
- Law no. 55/ 2001 for the ratification of the Additional Protocol of the Convention regarding Supervisory Authorities and Transborder Data Flows (4th of October 2001);
- Law no. 677/ 2001 regarding the protection of individuals with regard to the processing of personal data and the free movement of such data with completions and updates;
- Law no. 102/2005 regarding the setting up, organization and functioning of the National Supervisory Authority for Personal Data Processing;

### *Personal data protection in SIS – Art. 102 – 118 CAAS*

- G.E.O no. 128/2005 regarding setting up, organizing and functioning of the National IT System on Alerts;
- G.D. no. 1411/2006 on approving the Implementation rules of Government Emergency Ordinance no. 128/2005 on creating, organization and functioning of the National IT System for Alerts;
- Law. No. 345/2005 for approving the GEO no. 128/2005 regarding setting up, organizing and functioning of the National IT System on Alerts;

🔔 These normative acts are currently being amended in order to ensure the compatibility with the Community legislation in the field of SIS II, respectively the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);

🔔 The Recommendation no. R (87) 15 of the Committee of ministers to member states regulating the use of personal data in the police sector was transposed into national legislation;

## WHAT DOES THE SCHENGEN INFORMATION SYSTEM MEAN?

The Schengen Information System is an electronic data-base of police interest which allows the competent authorities to cooperate in order to maintain the public order, national security on the territories of member states, using data communicated via this system.

Currently, SIS reunites approx. 15 millions of alerts entered by the member states. All the member states enter data into the system directly from the national data-bases.

The current Schengen Information System was established for 18 states (15 member states, Iceland, Norway and an additional place), an architecture overtaken by the new configuration of the European Union.

The new technical discoveries, the new requires of the SIS during its operation, the new legal context subsequent to the Amsterdam Treaty and the enlargement of the European Union lead to the developing of SIS of second generation.

SIS II comprises a central system (C. SIS II), a national system (N. SIS) and a communication infrastructure between C. SIS and N.SIS. All national systems are connected online with the central system, located in Strasbourg.

As a preliminary step in the process of implementation of SIS II, National Information System of Alerts will be set up in our country, which contains the alerts of national interest and of Schengen interest entered by the competent national authorities.

NISA permits the competent authorities, through an automated search procedure in the system, to have access to alerts regarding persons or goods, in order to fulfill their specific attributions in the field of state border crossing checks, observing the customs regime, issuing visas and residence permits as well as other checks and specific activities carried out by the police staff or by other authorities in order to ensure the public order and national security.

## GENERAL RULES REGARDING DATA ENTERED IN SIS

Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities to carry out a direct search.

Data may not be used for administrative purposes.

Only the Member State issuing an alert shall be authorized to modify, add to or correct data which it has entered. Alerts in SIS may be accessed by all Schengen member states, respectively by the authorities' abilities by law within those member states.

Each member state shall ensure that each transaction of personal data is recorded into the national system of SIS by the management authority, in order to check the admissibility of the search.

Personal data entered in SIS is stored not longer than the period necessary to achieve the purpose for which it was entered.

At national level, all transactions made over the data in NISA are registered in the system in order to verify the legality of the search, monitor the legality over the processing of personal data and ensure the adequate functioning of NISA as well as the integrity and the security of the data.

The records regarding transactions may be used only for the purpose mentioned above and are deleted after a period of one year up to 3 years from their creation. The records may be kept for a longer period of time provided they are necessary for the monitoring procedures which are carried out at that moment.

All the statuses that alerts go through from the moment of their entering into NISA up to the moment of their deletion are recorded in the alerts history in order to monitor and verify the legality of the processing of data.

The records indicate the date and hour of the data transmission, data used for performing a search, a referral regarding the data transferred and the name of the competent authority and of the person that performed the data processing.

## PERSONAL DATA ENTERED IN SIS

☞ data regarding persons wanted for arrest for surrender purposes on the basis of an European Arrest Warrant and wanted for arrest for extradition purposes;

☞ data regarding citizens of third countries against whom the measure of forbidden the entrance or residence was disposed, according to art. 24, 25, 26 from the Regulation of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

☞ data regarding missing persons:

who need protection, on the basis of a decision issued by a competent authority, for the purpose of their own protection or to prevent a real threat;

who do not need protection but whose location needs to be determined;

☞ data regarding wanted persons in order to take part at a judiciary procedure, whose domicile or residence has to be established in the following cases:

- Persons subpoenaed as witnesses by the judicial authorities;
- Persons subpoenaed or wanted in order to be subpoenaed to appear in front of judicial authorities concerning a criminal procedure in order to account for deeds for which the criminal prosecution has been disposed;
- Persons to whom a court decision or other documents regarding a judicial procedure has to be delivered in order to account for deeds for which the criminal prosecution has been disposed;
- Persons to whom a subpoena shall be delivered in order to carry out a sentence depriving of liberty;

☞ data concerning persons who are subject to a discreet surveillance for the purpose of a criminal prosecution or to serve a sentence as well as for the prevention of threats to public order or national security;

#### ELEMENTS OF PERSONAL DATA ENTERED IN SIS

☞ surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately;

☞ any specific, objective, physical characteristics not subject to change;

☞ place and date of birth;

☞ sex;

☞ photographs;

☞ fingerprints;

☞ nationality;

☞ whether the person concerned is armed, violent or has escaped;

☞ reason for the alert;

☞ authority issuing the alert;

☞ a reference to the decision giving rise to the alert;

☞ action to be taken;

☞ link(s) to other alerts issued in SIS II;

☞ the type of offence.

**☞ The personal data users must access only personal data necessary for fulfilling the legal attributions**

## THE CONSENT OF THE PERSON WHOSE PERSONAL DATA IS PROCESSED

Any personal data processing, except for the processing of the data within the categories foreseen by the law, may be performed provided the data subject has given her express and unequivocal consent regarding that processing.

Within the exceptions provided by the law, we mention the situations in which the consent of the data subject is not necessary when the processing is performed:

- *when the processing is necessary in order to protect the life, physical integrity or the health of the data subject or of a third party who is at risk;*
- *when the processing is necessary in order to fulfill a legal obligation of the data-controller;*
- *when the processing is necessary in order to fulfill a public interest or which concerns the exercise of public official authority prerogatives with which the data – controller or the third party whom the data is disclosed is vested.*

## NATIONAL AUTHORITIES COMPETENT IN MANAGING AND EXPLOITING NISA

The Minister of Administration and Interior , by its special structure , is the central public authority which manages and is responsible for the good functioning of NISA, for the integrity of the alerts entered into NISA according to the provisions of the Schengen Acquis and in the same time it ensures the access of the national competent authorities to NISA.

The managing and use of data contained in NISA, regarding the processing of personal data, are subject to the verification of **National Supervisory Authority for Personal Data Processing (NSAPDP)**. At national level the National Supervisory Authority for Personal Data Processing is the public authority with legal personality, autonomous and independent of any other authority of public administration and of any natural or legal person within private sector. At the same time, it is the only authority with control attributions, investigation and supervision in the field. The president of NSAPDP, while exercising his attributions, issues compulsory decisions and instructions applicable to all the institutions and units to which the documents refer to.

The national authorities competent to enter data in NISA are those authorities who have attributions in providing and/or consulting the alerts contained in NISA. Presently, these authorities are foreseen in G.E.O. no 128/ 2005 *regarding* setting up, organizing and functioning of the National IT System on Alerts, as follows:

- ↳ Romanian Police;
- ↳ Romanian Border Police;
- ↳ Romanian Gendarmerie;
- ↳ Romanian Immigration Office;
- ↳ SIRENE Bureau, from the date of its operation;
- ↳ National Inspectorate for Persons Records;
- ↳ General Directorate for Passports;
- ↳ Directorate for Driving Licenses and Vehicles Registration Certificates;
- ↳ National Customs Authority;
- ↳ Ministry of Foreign Affairs;
- ↳ Ministry of Justice;

Competent national authorities consult only the alerts contained in NISA required in order to carry out its attributions and ensure the access only for the authorized personnel in the limits of the professional competences.

## SECURITY MEASURES FOR THE PROTECTION OF PERSONAL DATA

Each national competent authority is obliged to adopt necessary measures in order to ensure an adequate level of protection of personal data:

- a) to block access of unauthorized persons to the equipments for processing the personal data (access control to the equipment);
- b) prevent the unauthorized reading, copying, modification or removal of data media (data media control);
- c) prevent the unauthorized input of data and the unauthorized inspection, modification or deletion of stored personal data (storage control);
- d) prevent the use of automated data-processing systems by unauthorized persons using data communication equipments (user control);
- e) ensure that persons authorized to use an automated data-processing system have access only to the data covered by their access authorization (data access control);
- f) ensure that it is possible to verify and establish to which bodies' personal data may be transmitted using data communication equipments (communication control);
- g) ensure it is subsequently possible to verify and establish which personal data has been input into automated data-processing equipment (input control);
- h) prevent the unauthorized reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control).

## THE RIGHTS OF THE DATA SUBJECT IN THE CONTEXT OF PERSONAL DATA PROCESSING

According to the personal data principles, the rights of the data subjects are recognized by Schengen Convention.

Any person has the right to have access to the personal data included in SIS, according to the national legislation, if the persons request it.

Any person has the right to request from the authorities of control the verification of the personal data included in the Schengen Information System and the way the data has been used.

This right is stipulated by the national legislation of the Contracting Party which the request is addressed to. If the personal data was entered by another Contracting Party, the verification is performed in close cooperation with the authority of control of that Contracting Party.

The Constitution of Romania recognizes the rights of citizens to intimate, family and private life, irrespective of their nationalities, without a distinction between the Romanian citizens, foreign citizens and stateless persons who live in Romania.

The Law no.677/2001, with subsequent amendments and completions, stipulates the specific rights of the data subject in the context of personal data processing

☞ **Informing the data subjects** – *the data controller is obliged to inform the data subject regarding the processing of personal data.*

☞ **The right of access to data** – *any data subject has the right to obtain from the data controller, upon request, and free of charge ,once a year, the confirmation of the fact that the personal data is or is not being processed by the data controller.*

☞ **The right of intervention upon the data** – *any data subject has the right to obtain from the data controller, free of charge, the rectification, updating, blocking, or deletion of the data whose processing does not comply with the provisions of the law, notably of incomplete or inaccurate data;*

☞ **The right to object** – *the data subject has the right to object any time, by filing a written, dated and signed petition, based on justified and legitimate reasons linked to his particular situation that his or her personal data made the subject of the personal data processing.*

☞ **The right not to be subject to an individual decision** – *the withdrawal or the cancellation of a decision that produces legal effects concerning him/her, adopted exclusively on a personal data processing basis, carried out through automatic means,*

☞ **The right to refer to a Court of Law** – *any person who has suffered a prejudice as a consequence of an unlawful processing of personal data may address to the competent court of law in order to obtain compensation for the prejudice suffered.*

## EXEMPTION

The provisions referring to the right to information, the right of access to data, the right to object and the obligation of the data controller to communicate the name of the third person to whom the personal data has been revealed , do not apply to the processing and transfer of personal data, carried out within the activities of preventing, investigating and repressing criminal offences and maintaining public order, as well as of other activities in the field of criminal law, with the limitations and restrictions established by the law.

Thus, in the situation above, the law enforcement authorities are not obliged to inform the data subject about the processing of his personal data.

This exemption from the data controller's obligations is not permanent having in mind that the legal provisions are applicable only for the time necessary in order to achieve the goal intended by carrying out the activities mentioned above.

After the end of the situation, the data controller must take all the necessary measures in order to ensure the rights of the data subject in the context of personal data processing.

## SUBMITTING THE PETITION/PRINTED FORM BY A DATA SUBJECT REGARDING HIS DATA PROTECTION RIGHTS

Regarding to his/her rights, any person (petitioner) may directly address to the data controller through a written, dated and signed petition.

The petitioner may specify in the petition whether he/she wishes to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures personal receipt of the letter.

In case in which the petition is submitted by a legal representative, the identification data along with the mandate of the representative shall be requested.

The petition is submitted to the registrature of each data controller. In the same day, the petition is recorded in an entry-exit register of the correspondence and a number and data is allocated to the petition. The registration number and date of the petition filled in according to the above specifications may be communicated by the data controller at the express request of the petitioner.

## SOLVING THE PETITION SUBMITTED BY A DATA SUBJECT

The data controller is obliged to communicate the information requested, within 15 days from the receiving of the petition, observing the petitioner's option expressed in writing.

Regarding the data subject rights in the context of personal data processing in SIS, the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) stipulates that the interested person is informed as soon as possible, and in any case not later than 60 days from the date he/she submits the request of access and not later than 90 days for the right of intervention upon the data.

For example, in the case of exercising right of access, the data controller is obliged, in case he has processed any personal data concerning the petitioner, to communicate the petitioner, observing the legal term, along with the confirmation, at least the following:

- a) information regarding the purposes of the data processing, the categories of data concerned, and the recipients or the categories of recipients to whom the data are to be disclosed;
- b) communication in an intelligible form of the processed data and of any other available information regarding the source of origin of the respective data;
- c) information on the technical principles and mechanisms involved in the data processing concerning that data subject;

- d) information concerning the existence of the right of intervention upon the data, and the right to object, as well as the conditions in which the data subject can exert these rights;
- e) information on the possibility of consulting the Register of personal data processing, of submitting a complaint to the supervisory authority, as well as of disputing the data controller's decisions in court.

## INFORMING THE DATA SUBJECT ABOUT OTHER RIGHTS

The data controller informs the data subject of the right to refer to the Court of Law, in case he suffered a prejudice as consequence of unlawful processing of personal data without infringing the right of data subject to address directly to NSAPDP with a complaint.

The competent court of law is the one whose territorial jurisdiction covers the complainant's domicile. The complaint addressed to the court of law is free of charge.

The data controller shall inform the data subject about the right to address complaints directly to the NSAPDP in order to defend the personal data rights; thus, the data controller provides the data subject the following general information in order to contact NSAPDP (address, phone number, fax number, email address)

**Referring to the personal data contained in NISA, any interested person may request MoAI, according to the law, information regarding his/her personal data existing in NISA. Any prejudiced person may request for the legal redress of the prejudice caused by introducing or exploiting his/her personal data in NISA.**

## COMPLAINTS ADDRESSED TO THE NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING

If the person whose personal data processing considers the rights stipulated by the Law. No. 677/2001 have been breached, he may file in a complaint to the national supervisory authority. The complaint submitted to the supervisory authority is invalid if a claim, concerning the same matter and parties, was previously submitted to a court of law. The person must previously address to the data controller.

The complaint may be addressed directly or through a representative to the National Supervisory Authority. The data subject may empower an association or a foundation to represent his/her interests.

Except for the cases in which a delay would cause an imminent or irreparable damage, the complaint submitted to the supervisory authority may not be addressed earlier than 15 days from submitting a similar complaint to the data controller.

If the complaint is well – founded, NSAPDP may issue a decision, in case it ascertains the infringement of the law, disposing the temporary suspension or cessation of the personal data processing, the partial or total erasure of the processed data. The motivated decision will be communicated to the interested parties within no longer than 30 days from the registration of the complaint.

The supervisory authority may address to a court of law in order to defend the rights of the data subjects.

For more details on data protection, please visit the NSAPDP website- [www.dataprotection.ro](http://www.dataprotection.ro).

## GENERAL INFORMATION ABOUT SCHENGEN AREA



### **I. What is Schengen?**

**Schengen** is a small border town in Luxembourg. In 1985, an agreement on the gradual abolition of checks at common borders between the Federal Republic of Germany, the French Republic, the Netherlands, the Kingdom of Belgium, the grand Duchy of Luxembourg was concluded, on the “Astrid” ship, on Mosel River, near Schengen.

### **II. What does Schengen area mean?**

An area of freedom of movement where the controls at internal borders of the Members States have been abolished and a single external border where the checks follow a strict set of rules was created.

### **III. Brief history of Schengen area**

- at the beginning of 80's at European level, a discussion on the importance of the term “free movement” started;
- 1985 – conclusion of the agreement between the Federal Republic of Germany, the French Republic, the Kingdom of Netherlands, the Kingdom of Belgium, the grand Duchy of Luxembourg;
- 19 June 1990 – signing of the Convention Implementing of the Schengen Agreement;
- 1995 – entering into force of the Convention Implementing of the Schengen Agreement.

### **IV. Schengen Member States**

French Republic, Kingdom of Belgium, Federal Republic of Germany, the grand Duchy of Luxembourg, Kingdom of Netherlands, Portugal Republic, Kingdom of Spain, Republic of Austria, Italian Republic, Hellenic Republic, Kingdom of Denmark, Republic of Finland, Republic of Iceland, Kingdom of Norway, Czech Republic, Republic of Estonia, Republic of Latvia, Republic of Lithuania, Republic of Malta, Republic of Poland, Slovak Republic, Republic of Slovenia, Kingdom of Sweden, Republic of Hungary, Swiss Confederation.

### **V. Future Member States of Schengen Agreement**

Republic of Cyprus, Principality of Liechtenstein, Republic of Bulgaria, Romania.

### **VI. Benefits of the accession to the Schengen area**

- Lifting of controls between internal borders of Schengen Member States
- Freedom of movement for citizens of Member States
- A set of measures in order to compensate the negative impact of abolition of controls at internal borders

For more details regarding Schengen area, please visit the Romanian website dedicated to Schengen [www.schengen.mai.gov.ro](http://www.schengen.mai.gov.ro).

## Definitions

**personal data-** any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity;

**personal data processing-** any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction;

**data controller-** any natural or legal person, including public authorities, institutions and their legal bodies, that establishes the means and purpose of the personal data processing; if the purpose and means of the personal data processing is set out or based on a legal provision, the data controller shall be the natural or legal person assigned as data controller by that specific legal provision;

**NISA-** National Information System of Alerts, compatible with SIS II, which contain alerts of national interest and Schengen interest transmitted by the national competent authorities;

**alerts-** set of data included in NISA related to persons or goods identified or identifiable that must be the object of certain measure disposed by a competent authority, according to the law, with a view to respecting the public interest, the free movement of persons and goods or, if the case, to ensuring the order and public safety and the prevention of the threats to the national security;

**National alerts-** an alert transmits by a national competent authority from its informatics' system in NISA

**Schengen alerts-** the alert entered in NISA and transmitted to SIS II

**National competent authorities-**the authorities with responsibilities in supplying the alerts in NISA, respectively SIS II and/or consulting the alerts contained in NISA and established by Government Decision;

**Schengen Information System (SIS)** – a common information system which permits the competent authorities within Member State to cooperate in order to maintain public order and national security on the territory of the Member State, using the information communicated through this system;

**SIS II-** second generation of SIS composed by central SIS II, a national system NSIS II in each Member State and a communication infrastructure which ensures the connection of the NSIS II to central SIS II;

**NSIS II** – Romanian national component of SIS II composed of NISA and national copy of SIS II

**National copy of SIS II-** the complete or partial copy of SIS II database, accessible for the purpose of performing automated searches in the territory of each of the Member States; SIS II central ensures automatically update of the national copy of SIS II, synchronization consistence between national copy and SIS II database, as well as its initialization and rehabilitation.