PERSONAL DATA PROCESSING IN SIS

AND EXERCISE OF THE RIGHTS OF THE DATA SUBJECTS

The Schengen area encompasses most of the European countries that have abolished their internal borders while providing a single set of rules for controls at the external borders, mostly functions as a single jurisdiction under a common visa policy for international travel purposes and providing cooperation in criminal matters between law enforcement and judicial authorities.

The Schengen Information System (Second Generation – SIS II) is the basis of cooperation in the Schengen area. With its help, the national border control authorities, as well as customs and police authorities (in charge with external, as well as Schengen border control) can send alerts regarding wanted or missing persons, as well as objects. Thus, SIS II plays an important role in compensating for the abolition of the internal border controls and facilitates the free movement of people in the Schengen area.

Only the national competent authorities such as law enforcement/judicial/administrative authorities have access to SIS II. They can access the data needed, in strict accordance to the purpose of carrying auto their tasks. European agencies EUROPOL and EUROJUST have limited access rights to carry out certain types of enquiries.

The SIS II is composed of: a central system based in Strasbourg, a national system in each Member State and a communication infrastructure between the central system and the national systems providing an encrypted virtual network dedicated to SIS II data and the exchange of data between the authorities.

In Romania, it was established the **National Signaling Information System (SINS),** which contains the **alerts of both national and Schengen interest**, issued by competent national authorities. **SINS allows those authorities, through an automatic search procedure, to gain access to alerts** regarding persons and objects, in order to fulfill specific duties in areas such as state crossing border control, compliance with the customs regime, issuing visas and permits of residence, as well as other specific activities carried out by the law enforcement authorities in order to ensure public order and national security.

The Ministry of Internal Affairs, through its specialized structure, is the central public authority that manages and is responsible for the proper functioning of the SINS, for the accuracy of alerts introduced, according to the requirements of the Schengen acquis, ensuring the access of the competent Romanian authorities to the SINS

At the level of the **General Inspectorate of the Romanian Police (I.G.P.R)** functions the **International Police Cooperation Center (C.C.P.I)**, the national authority in the field of international police cooperation. At the level of C.C.P.I. the **SIRENE Bureau** is the human interface of the SIS, being **the only contact point with other member states and associates states.** It has as its main specific role the responsibility of providing information in real time, with the possibility of completing the information existent with additional data on a short notice. The SIRENE Bureau works as a dispatcher, available 24/7, to ensure the continuity of the flow of information between the equivalent national offices. SIS being a **hit/no-hit system**, **the alerts are brief**. Starting from input until discovery, **the necessary additional information** (other data that may be requested by SIS users in addition to what it is already provided, in order to carry out specific tasks) is received/transmitted by the SIRENE Bureau in the form of electronic standardized forms.

PROCESSING OF PERSONAL DATA IN SIS

Personal data are processed in SIS from the introduction of an alert related to a person until the deletion of the alert from the system. Throughout this entire period, the data may be consulted (e.g. when the person passes an external border or is stopped on a country's territory by law enforcement officers for a police check) or passed on to the beneficiary (when additional information is requested).

SIS PROCESSED DATA CATEGORIES

Types of data which can be processed in SIS are provided in:

a) **Regulation (EU) 2018/1860** of the European Parliament and of the Council of 28 November 2018 on the use of the **Schengen Information System for the return of illegally staying third-country nationals**, hereinafter designated as **Regulation SIS Returns**;

b) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the **Schengen Information System (SIS) in the field of border checks**, and amending the convention implementing the Schengen agreement, and amending and repealing Regulation (EC) no. 1987/2006, hereinafter designated as **Regulation SIS Border Checks;**

c) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the **Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters**, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) no. 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, hereinafter designated as **Regulation SIS Cooperation**.

SIS only contains data categories provided by each Member State and associated state and which are necessary to carry out their lawful tasks (art. 4 of Regulation no. 2018/1860 and art. 20 of Regulations no. 2018/1861 and 2018/1862).

Regulation (EU) 2018/1860

Article 4. (1) **An alert on return entered into SIS** in accordance with Article 3 of this Regulation **shall contain only the following data**:

(a) surnames; (b) forenames; (c) names at birth; (d) previously used names and aliases; (e) place of birth; (f) date of birth; (g) gender; (h) any nationalities held; (i) whether the person concerned: (i) is armed; (ii) is violent; (iii) has absconded or escaped; (iv) poses a risk of suicide; (v) poses a threat to public health; or (vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541; (j) the reason for the alert; (k) the authority which created the alert; (l) a reference to the decision giving rise to the alert; (m) the action to be taken in the case of a hit; (n) links to other alerts pursuant to Article 48 of Regulation (EU) 2018/1861; (o) whether the return decision is issued in relation to a third-country national who poses a threat to public policy, to public security or to national security; (p) the type of offence; (q) the category of the person's identification documents; (r) the country of issue of the person's identification documents; (s) the number(s) of the person's identification documents; (t) the date of issue of the person's identification documents; (u) photographs and facial images; (v) dactyloscopic data; (w) a copy of the identification documents, in colour wherever possible; (x) last date of the period for voluntary departure, if granted; (y) whether the return decision has been suspended or the enforcement of the decision has been postponed, including as a result of the lodging of an appeal; (z) whether the return decision is accompanied by an entry

ban constituting the basis for an alert for refusal of entry and stay pursuant to point (b) of Article 24(1) of Regulation (EU) 2018/1861.

The minimum set of data needed to introduce an alert are stated at (a), (f), (j), (l), (m), (x) and (z). The rest of the data are also registered in SIS if available.

Regulation (UE) 2018/1861

Article 20 (2) Any alert in SIS which includes information on persons shall contain only the following data:

a) surnames; b) forenames; c) names at birth; d) previously used names and aliases; e) any specific, objective, physical characteristics not subject to change; f) place of birth; g) date of birth; h) gender; i) any nationalities held; j) whether the person concerned: i) is armed, ii) is violent, iii) has absconded or escaped, iv) poses a risk of suicide, v) poses a threat to public health or vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU)2017/541; k) the reason for the alert; l) the authority which created the alert; m) a reference to the decision giving rise to the alert; n) the action to be taken in the case of a hit; o) links to other alerts pursuant to Article 48; p) whether the person concerned is a family member of a citizen of the Union or other person who is a beneficiary of the right of free movement as referred to in Article 26; q) whether the decision for refusal of entry and stay is based on: i) a previous conviction as referred to in point (a) of Article 24(2); ii) a serious security threat as referred to in point (b) of Article 24 (2); iii) circumvention of Union or national law on entry and stay as referred to in point (c) of Article 24 (2); iv) an entry ban as referred to in point (b) of Article 24 (1); v) a restrictive measure referred to in Article 25; r) the type of offence; s) the category of the person's identification documents; t) the country of issue of the person's identification documents; u) the number(s) of the person's identification documents; v) the date of issue of the person's identification documents; w) photographs and facial images; x) dactyloscopic data; y) a copy of the identification documents, in color wherever possible.

Regulation (UE) 2018/1862

Article 20 (2) The categories of data shall be as follows:

(a) information on persons in relation to whom an alert has been entered;

(b) Information on objects referred to in Articles 26, 32, 34, 36 and 38.

(3) Any alert in SIS which includes information on persons shall contain only the following data:

a) surnames; b) forenames; c) names at birth; d) previously used names and aliases; e) any specific, objective, physical characteristics not subject to change; f) place of birth; g) date of birth; h) gender; i) any nationalities held; j) whether the person concerned: i) is armed, ii) is violent, iii) has absconded or escaped, iv) poses a risk of suicide; (v) represents a threat to public health; or (vi) is involved in an activity mentioned in the articles 3-14 of the Directive (UE) 2017/541; k) the reason for the alert; l) the authority which created the alert; m) a reference to the decision giving rise to the alert; n) the action to be taken in case of a hit; o) links to other alerts pursuant to Art. 63; p) the type of offence; q) the person’s registration number in a national register; r) for alerts referred to in Art. 32 (1), a categorization of the

type of case, s) the category of the person's identification documents; t) the country of issue of the person's identification documents, u) the number(s) of the person's identification documents, v) the date of issue of the person's identification documents, w) photographs and facial images; x) in accordance with Art. 42 (3), relevant DNA profiles; y) dactyloscopic data; z) a copy of the identity documents, in color wherever possible.

Alerts introduced in SIS refer to:

- Warning notices imposing a ban on entry and stay
- Missing/Vulnerable persons whose travel should be prevented
- Alerts for persons wanted for the purpose of cooperation in court proceedings
- Alerts regarding persons and objects to be subject to covert or targeted control
- Alerts for items intended for seizure or use as evidence in criminal proceedings:
- Unknown circled persons
- Alerts for third-country nationals subject to expulsion decisions issued by Schengen countries.;
- Warnings concerning third-country nationals who are not entitled to enter or stay in the Schengen area.

AUTHORITIES THAT HAVE ACCESS TO SIS II

- Law enforcement authorities (national police/ national border police)
- National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge
- Authorities responsible for issuing visas, central authorities responsible for examining visa applications and authorities responsible for issuing residence permits
- Services responsible for issuing vehicle/other types of objects registration certificates

PERSONAL DATA PROTECTION IN SIS

Each member state as well as associated states apply their own rules of confidentiality for the ones working with SIS data and other supplementary information (persons as well as agencies) in accordance with their own domestic law. Data processing in the SIS System is carried out in accordance with European and national data protection rules.

The data may only be used for the purposes specified within each category of reporting. The data can only be copied for technical purposes and cannot be used for administrative purposes. Exceptions are punctual.

Before being authorized to process the data stored in SIS and periodically, after granting access to that data, the staff of the authorities that have the right to access the system benefit from appropriate training on data security, fundamental rights (data protection), rules and procedures of data processing.

Any access and exchanges of personal data from the SIS database are recorded in N. SIS for the purpose of verifying the legality of the search, of the data processing, self-monitorization and ensuring the proper functioning of the N SIS, as well as data integrity and security. The recordings may only be used for the

aforementioned purposes and are deleted after three years. The ones that include the history of the alerts are deleted three years after the deletion of the alerts

THE RIGHTS OF DATA SUBJECTS

The rights of the data subjects (as laid down in art. 19 of Regulation (UE) nr. 2018/1860, art. 53 of Regulation (UE) nr. 2018/1861 and art. 67 of Regulation (UE) nr. 2018/1862) are:

- **Access to the personal data** - the data subject has the right to know whether his data are registered or not in the SIS
- **The right to rectify inaccurate data** – the data subject has the right to request the correction of the erroneous data from the SIS
- **The right to erase illegally stored data** – the data subject has the right to request data deletion if it is permitted by law

EXERCISE OF THE RIGHTS OF THE DATA SUBJECTS

The rights of access, rectification and erasing of data in the context of processing personal data in the SIS are exercised, as the case may be, according to:

- **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)
- **Law no. 363/2018** on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

To exercise these rights (right of access, right of rectification, right of erasing), **the data subject can**:

- **send/submit an application to the headquarters of the General Inspectorate of the Romanian Police** in Bucharest, district 5, Mihai Vodă street, no. 6, postal code 030167;
- **submit an electronic request to the General Inspectorate of the Romanian Police at the e-mail** address: **ccpi@mai.gov.ro**

The requests submitted/ transmitted to **any data operator within the Ministry of Internal Affairs** (Border Police website **www.politiadefrontiera.ro**, Immigration Office **igi.mai.gov.ro** , and others) will be sent to the SIRENE Bureau within 5 days from their receipt, according to Law no.141/2010 on the establishment, organization and operation of the National Signaling Information System and Romania's contribution to the Schengen Information System, republished (this normative act is to be repealed by a law establishing the preliminary measures, conditions and procedures regarding the introduction and processing of the data of national interest in the SINS, as well as in the national application of certain provisions contained in the Regulation (EU) no.2018/1860,2018/1861, 2018/1862)

Sample applications can be found at the end of the current page

Requests for rectification and/or erasing must necessarily include the personal data whose rectification and/or erasing is requested.

Applications must be signed by the person whose data was processed and are considered valid only if proof of identity is provided (a copy of an identity document). If the data subject is represented by a lawyer, the application must be signed by both the data subject and the lawyer, and must be accompanied by the power of attorney, as well as a copy of an identity document of the data subject.

RESOLUTION OF CLAIMS

The SIRENE Bureau, within the General Inspectorate of the Romanian Police is the only authority in Romania authorized to respond to these requests. **It has the obligation to communicate to the person concerned information regarding the actions taken following a request submitted** pursuant to art. 15, 16, 17 of Regulation (EU) 2016/679, respectively art. 16 and 18 par. 1, 3 of Law no. 363/2018, **as soon as possible, but not later than 60 days from the date of receipt of the request, in the case of exercising the right of access to personal data, and as soon as possible, but not later than 90 days from the date upon receipt of the request, in the case of exercising the right to rectification and removal of personal data** (according to art. 62, paragraph 2 of Law no. 141/2010).

If the data subject submits **the request electronically**, the information is provided also electronic format where possible, unless the data subject requests another format.

Any communication and any measures taken are offered by I.G.P.R. free of charge. If requests from a data subject are unfounded or excessive, in particular due to their repetitive nature, the I.G.P.R. may be:

- 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.

EXCEPTIONS REGARDING THE EXERCISE OF RIGHTS (art. 19 of Regulation (EU) 2018/1860, art. 53 of Regulation (EU) 2018/1861 and article 67 of Regulation (EU) 2018/1862)

A Member State in accordance with its national law, **shall take a decision not to provide information to the data subject,** in whole or in part, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; or (e) protect the rights and freedoms of others.

The Member State informs the data subject of the possibility to file a complaint with the supervisory authority or to initiate a judicial appeal.

APPEAL (art. 19 of Regulation (UE) 2018/1860, art. 54 of Regulation (UE) 2018/1861 and Art. 68 of Regulation (UE) 2018/1862)

Without prejudice to the provisions on remedies of Regulation (EU) 2016/679 and of Directive (EU) 2016/680, **any person may bring an action before any competent supervisory authority or a court**, under the law of any Member State to access, rectify, erase, obtain information or obtain compensation in connection to an alert relating to him or her.

Right to lodge a complaint to a supervisory authority (Article 77 of EU Regulation 2016/679, Article 57 of Law No. 363/2018)

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 EU Regulation 2016/679 or Law No. 363/2018.

Contact details of the National Authority for the Supervision of Personal Data Processing (A.N.S.P.D.C.P.):

Headquarters: B-dul G-ral Gheorghe Magheru 28-30,distric 1, zip code 010336, Bucharest

Telephone: 031.805.92.11; Fax: 031.805.96.02

Website: **www.dataprotection.ro** E-mail: **anspdcp@dataprotection.ro**

To file a complaint to A.N.S.P.D.C.P. click aici

Right to an effective judicial remedy against a controller or processor (Pursuant to art.79 of Regulation (EU) 2016/679 and art. 58 of Law nr. 363/2018)

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that their rights under the Regulation UE 2016/679 or Law no. 363/2018, have been infringed as a result of the processing of their personal data in non-compliance with these two legal acts.

SAMPLES OF REQUESTS FOR THE EXCERCIZE OF THE RIGHTS

REQUEST/APPLICATION FOR THE EXERCISE OF THE RIGHT OF ACCESS

To

GENERAL INSPECTORATE OF THE ROMANIAN POLICE
Bucharest, 4-6 Mihai Vodă street, district 5

The undersigned ..... (name and surname), domiciling/residing in ..... str. ..... no. ....., county/district..... (PIN) personal identification no..... telephone no. ....., email address (optional)....., pursuant to art. 16 of the Law nr. 363/2018, kindly ask you to inform me if my personal data has been processed by your institution, during the period ……, in the Schengen Information System.

(optional) Request is submitted through a representative (identification data of the representative)……, correspondingly I submit the power of attorney/notarial power of attorney for the representative (the appropriate option is selected).

The answer shall be provided to my domicile/residence address or electronically, to the email address:……

Pursuant to art. 12 (10) of the Law nr. 363/2018, to prove my identity, I send you attached, the copy of my ID.

I hereby declare that all the information provided above is true and correct.

Date Signature

REQUEST FOR THE EXCERCISE OF THE RIGHT OF DATA RECTIFICATION

To

GENERAL INSPECTORATE OF THE ROMANIAN POLICE
Bucharest, 4-6 Mihai Voda street, district 5

The undersigned ..... (name and surname), domiciling/residing in ..... str. ..... nr. .....…… county/district..... (PIN) personal identification nr..... telephone nr. ....., email address (optional)....., pursuant to art. 18 of the Law nr. 363/2018, kindly ask you to undertake the necessary legal measures for the rectification of the following personal data, regarding:……(shall be enumerated the data to be rectified). My request is determined by the following reasons:……..(shall be mentioned the reasons). (optional) Request is submitted through a representative (identification of the representative)……, correspondingly I submit attached, the power of attorney/notarial power of attorney of the representative (the appropriate option is selected).

The answer shall be provided at my domicile/residence address or electronically, by email:……

Pursuant to art. 12 (10) of the Law no. 363/2018 in order to prove my identity, I attached a copy of my ID

I hereby declare that all the information provided above is true and correct.

Date Signature

REQUEST FOR THE EXCERCISE OF THE RIGHT TO PERSONAL DATA DELETION

To

GENERAL INSPECTORATE OF THE ROMANIAN POLICE
Bucharest, 4-6 Mihai Voda street, district 5

The undersigned ..... (name and surname), domiciling/residing in ..... str. ..... nr. …….. county/district..... (PIN) personal identification nr..... telephone nr. ....., email address (optional)....., pursuant to art. 18 (3) of the Law nr. 363/2018, kindly ask you to undertake the necessary legal measures for the erasure of the following personal data, regarding:……(shall be enumerated the data to be erased). My request is determined by the following reasons: data is no longer necessary for the fulfillment of the purpose for which they were collected or processed/I withdraw my consent/they were processed illegally/compliance with a legal obligation that falls under your competence (the appropriate option is mentioned).……..

(optional)This Request is submitted through a representative (the identification data of the representative)……, correspondingly I submit attached, the notarial power of attorney of the representative (the appropriate option is selected).

The answer to my request shall be sent to my residence/domicile address, or electronically, by email……..

Pursuant to art. 12 (10) of the Law no 363/2018 in order to prove my identity, I attached a copy of my ID

Hereby, I declare that all the information provide above is true and correct.

Date Signature

* The time necessary to fill in the request for the exercise of rights may vary depending on the additional information the applicant wishes to provide. The standard time to fill in the form is approximately 2 minutes.

CONTACT DETAILS OF THE UNIT RESPONSIBLE WITH DATA PROTECTION

General Inspectorate of the Romanian Police/ Personal Data Protection Unit

Headquarters: Bucharest, district 2, 13-15 Șoseaua Ștefan cel Mare

e-mail: **cpdcp@politiaromana.ro**; Telephone nr.: +4021 208 25 25 (int. 26559).

Updated on 29.08.2022