THE SCHENGEN INFORMATION SYSTEM

A GUIDE FOR EXERCISING THE RIGHT OF ACCESS

I. INTRODUCTION TO THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II)

The SIS II is a large-scale IT system, set up as a compensatory measure for the abolition of internal border checks, and intends to ensure a high level of security within the area of freedom,security and justice of the European Union, including themaintenance of public security and public policy and the safeguardingof security in the territories of the Member States.The SIS II is already implemented in all EU Member States, with the exception of Cyprus, Croatia and Ireland[1], and in four Associated States: Iceland, Norway, Switzerland and Liechtenstein.

The SIS II is an information system that allows national law enforcement, judicial and administrative authorities to perform specific tasks by sharing relevant data. The European agencies EUROPOL and EUROJUST also have limited access privileges to this system.

Categories of information processed

SIS II centralises two broad categories of information taking the form of alerts on, firstly, *persons* - who are either wanted for arrest, missing, sought to assist with a judicial procedure, for discreet or specific checks, or third country nationals subject to refusal of entry or stay in the Schengen area, and, secondly, *objects* - such as vehicles, travel documents, credit cards, for seizure or use as evidence in criminal proceedings, or for discreet or specific checks.

[1] Information dated from July 2015. Though operating the SIS, Bulgaria and Romania still have internal borders. The UK has access to the SIS except for alerts for purposes of non-admission to the Schengen territory.

Legal basis

Depending on the type of alert, the SIS II is regulated either by Regulation (EC) 1987/2006 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 with respect to alert procedures falling under Title IV of the Treaty establishing the European Community (former first pillar)[2] or by Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System in what concerns procedures falling under Title VI of the Treaty on European Union (former third pillar)[3].

Categories of personal data processed

When the alert concerns a person, the information must always include the name, surname and any aliases, the sex, a reference to the decision giving rise to the alert and the action to be taken. If available, the alert may also contain information such as any specific, objective, physical characteristics not subject to change; the place and date of birth; photographs; fingerprints; nationality(ies);whether the person concerned is armed, violent or has escaped; reason for the alert; the authority issuing the alert; links to other alerts issued in SIS II in accordance with Article 37 of SIS II Regulation or Article 52 of SIS II Decision.

Architecture of the system

The SIS II is composed of:

•a central system ("Central SIS II");

•a national system (the "N.SIS II") in each Member State (the national data systems that will communicate with the Central SIS II);

•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 responsible for the exchange of all supplementary information * (SIRENE Bureaux)[4].

[2] Hereinafter, 'SIS II Regulation'.

[3] Hereinafter, 'SIS II Decision'.

[4] SIS II data is entered, updated, deleted and searched via the various national systems. The central system, which performs technical supervision and administration functions, is located in Strasbourg (France). It provides the services for the entry and processing of SIS II data. A backup central system, capable of ensuring all functionalities of the principal central system in the event of failure of this system, is located near Salzburg (Austria). Each Member State is responsible for setting up, operating and maintaining its own national system and for connecting it to the central system. It designates an authority, the national SIS II office (N.SIS II office), which has central responsibility for its national SIS II project. This authority is responsible for the smooth operation and security of its national system.

II. RIGHTS RECOGNIZED TO INDIVIDUALS WHOSE DATA IS PROCESSED IN THE SIS II

In accordance with data protection principles, all individuals whose data is processed in the SIS II are recognised specific rights[5]by the aforementioned SIS II Decision and Regulation.

These are basically:

- the right of access to data relating to them stored in the SIS II;
- the right to correction of inaccurate data or deletion when data have been unlawfully stored;
- the right to bring proceedings before the courts or competent authorities to correct or delete data or to obtain compensation[6].

Anyone exercising any of these rights can apply to the competent authorities in the Schengen State of his choice. This option is possible because all national databases (N.SIS II) are identical to the central system database (CS.SIS)[7]. Therefore these rights can be exercised in any Schengen country regardless of the State that issued the alert.

When an individual exercises his right of access, correction of inaccurate data and deletion of unlawfully stored data, replies by competent authorities are due within a strict deadline. Thus, the individual shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access, or sooner if national law so provides[8].

Also the individual shall be informed about the follow-up given to the exercise of his rights of correction and deletion as soon as possible and in any event not later than three months from the date on which he applies for correction or deletion, or sooner if national law so provides[9].

II.1. **Right of access**

The right of access is the possibility for anyone who so requests to have knowledge of the information relating to him stored in a data file as referred to in national law. This is a fundamental principle of data protection which enables data subjects to exercise control over personal data kept by third parties.

[5] See in particular Article 41 of SIS II Regulation and 58 of SIS II Decision
[6] See Article 43 of SIS II Regulation and 59 of SIS II Decision
[7] See Article 4(1)(b) of SIS II Regulation and Decision.
[8] See Article 41(6) of SIS II Regulation and 58(6) of SIS II Decision.
[9] See Article 41(7) of SIS II Regulation and 58(7) of SIS II Decision

This right is expressly provided for in Article 41 of SIS II Regulation and in article 58 of SIS II Decision[10].

The right of access is exercised in accordance with the law of the Member State where the request is submitted. The procedures differ from one country to another, as well as the rules for communicating data to the applicant. When a Member State receives a request for access to an alert not issued by itself, that State must give the issuing country the opportunity to state its position as to the possibility of disclosing the data to the applicant[11].

The information shall not be communicated to the data subject if this is indispensable for the performance of the legal task connected to the alert, or in order to protect the rights and freedoms of other people.

Also there are currently two types of system governing the right of access to data processed by law enforcement authorities, and thus also applicable to SIS data. In some Member States the right of access is direct, in others it is indirect.

II.1.1. Direct access

In this case the person concerned applies directly to the authorities processing the data (police, *gendarmerie*, customs, etc.). If national law permits, the applicant may be sent the information relating to him..

II.1.2. Indirect access

In this case the person applies for access to the national data protection authority of the State where the request is submitted. The data protection authority conducts the necessary verifications to handle the request and provides a reply to the applicant.

[10] Both Articles state : 'The right of persons to have access to data relating to them entered in SIS II in accordance with this regulation shall be exercised in accordance with the law of the Member State before which they invoke that right.[…]'

[11] See Articles 41(3) of SIS II Regulation and 58(3) of SIS II Decision

II.2. **Right to correction and deletion of data**

Besides the right of access, there are also the right to obtain the correction of personal data factually inaccurate or incomplete or the right to ask for deletion of personal data unlawfullystored (Article 41(5) of SIS II Regulation and 58(5) of SIS II Decision).

Under the Schengen legal framework only the Member State responsible for issuing an alert in the SIS may alter or delete it (See Article 34(2) of SIS II Regulation and 49(2) of SIS II Decision).

If the request is submitted in a Member State that did not issue the alert, the competent authorities of the Members States concerned cooperate to handle the case, by exchanging information and making the necessary verifications.

The applicant should provide the grounds for the request to correct or delete the data and gather any relevant information supporting it.

II.3. **Remedies: the right to complain to the data protection authority or to initiate a judicial proceeding**

Articles 43 of SIS II Regulation and 59 of SIS II Decision present the remedies accessible to individuals when their request has not been satisfied. Any person may bring an action before the courts or the authority competentunder the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him.

In case they have to deal with a complaint with a cross-border element, DPAs should cooperate with each other to guarantee the rights of the data subjects.

III. DESCRIPTION OF THE PROCEDURE FOR THE EXERCISE OF THE RIGHT OF ACCESS IN EACH CONCERNED STATE

ROMANIA

1. Nature of right of access

The right of access in Romania is direct.

2. Contact detail of the body to which requests for access should be addressed

According to Article 62 (3) of Law no. 141/2010 on the setting up, organisation and functioning of the National Information System for Alerts (NISA) and participation of Romania to the Schengen Information System, the requests may be submitted to the national SIRENE Bureau or to any data controller within the Minister of Administration and Interior or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

Address for correspondence:
Centre for International Police Cooperation
SIRENE Bureau
1-5 Calea 13 Septembrie, Bucharest, 5th District
Romania
Tel.: +40 21 315 96 26
Tel.: +40 21 314 05 40
Fax: +40 21 314 12 66
Fax: +40 21 312 36 00
E-mail: ccpi@mai.gov.ro

3. Formalities for the request: information and documents to be supplied/possible costs

The rights of the person as regards the personal data processing in the NISA or SIS II are used according to the provisions of Law no. 677/2001 on the protection of individuals with regard to the personal data processing and the free movement of such data, with the subsequent modifications and amendments, with the exceptions mentioned by this law.

According to Article 13 (1) of Law no. 677/2001, *an application for access is free of charge.*
The data subject shall not be communicated information regarding personal data processed in NISA or SIS II as long it is necessary for performing the activities on the basis of the alert or the objective of the alert or for protecting the rights and freedom of other persons.

4. Contact details of the national data protection authority and its possible role

The legality of the personal data processing in the N.SIS on the territory of Romania and transmitting this data abroad, as well as subsequent exchanging and processing of supplementary information are subject to monitoring and control by the National Supervisory Authority for Personal Data Processing.

The auditing of the personal data processing is performed by the National Supervisory Authority for Personal Data Processing according to audit international standards at least once every four years.

Address for correspondence:
National Supervisory Authority For Personal Data Processing
28-30 G-ral Gheorghe Magheru Bld.
Bucharest, 1st district 1
Romania
Tel.: +40 31 805 9211
Fax: +40 31 805 96 02
E-mail: anspdcp@dataprotection.ro

5. Expected outcome of the requests for access. Content of the information supplied

The requests of the data subjects in the context of personal data processed in the NISA or the SIS II can be submitted only to the national SIRENE Bureau which will communicate the answer to the applicant as soon as possible but no later than 60 days after the receipt of the request, in the case of using the right of access to the personal data and as soon as possible but no later than 90 days after the receipt of the request in the case of using the right of rectification and deletion of the personal data, by exception from the provisions of Law no. 677/2001, with the subsequent modifications and amendments.

6. References of the main national laws that apply

- Law no. 141 of 12th of July 2010 on the setting up, organisation and functioning of the National Information System for Alerts (NISA) and participation of Romania to the Schengen Information System,
- Law no. 677 of 21st of November 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed.

7. Language regime

If the data subject is Romanian, he/she can submit his/her request in Romanian and if the data subject is foreigner, he/she can submit his/her request in English.