Schengen Information System II - A Guide for Exercising the Right of Access
Summary

Persons whose personal data are collected, held or otherwise processed in the second generation Schengen Information System (hereinafter 'SIS II') are entitled to rights of access, correction of inaccurate data and deletion of unlawfully stored data[1]. This Guide describes the modalities for exercising those rights.

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 the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States. The SIS II is implemented in all EU Member States, with the exception of Cyprus, Croatia and Ireland[2], 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.

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 (hereinafter "SIS II Regulation") or by the 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 (hereinafter "SIS II Decision").

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,

[1] These rights are granted under Articles 41 of Regulation (EC) n°1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Article 58 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

[2] 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.

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 (1) a central system ("Central SIS II"), (2) a national system (the "N.SIS II") in each Member State, that will communicate with the Central SIS II and (3) 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)[3].

II. Rights granted to individuals whose data are processed in the SIS II

In accordance with data protection principles, all individuals whose data are processed in the SIS II are granted specific rights by the SIS II Regulation and the SIS II Decision[4], which will be analysed below. Anyone exercising any of these rights can apply to the competent authorities in the State of his choice where SIS II is operated. This option is possible because all national databases (N.SIS II) are identical to the central system database[5]. Therefore these rights can be exercised in any country that operates SIS II, regardless of the Member 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[6]. 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.[7].

Right of access

The right of access is the possibility for anyone who so requests to have knowledge of the information relating to him or her 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. This right is expressly provided for in Article 41 of SIS II Regulation and in Article 58 of SIS II Decision.

---

[3] 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.

[4] See in particular Article 41 of SIS II Regulation and 58 of SIS II Decision.

[5] See Article 4(1)(b) of SIS II Regulation and Decision.

[6] See Article 41(6) of SIS II Regulation and 58(6) of SIS II Decision.

[7] See Article 41(7) of SIS II Regulation and 58(7) of SIS II Decision

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[8]. The information shall not be communicated to the data subject if it 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.

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.

In the case of **direct access**, the person concerned applies directly to the authorities handling the data (police, *gendarmerie*, customs, etc.). If national law allows, the applicant may be sent the information relating to him.

In the case of **indirect** access, the person sends his or her request for access to the national data protection authority of the State to which the request is submitted. The data protection authority conducts the necessary verifications to handle the request and replies to the applicant.

Right to correction and deletion of data

The right of access is complemented by the right to obtain the correction of the personal data when they are factually inaccurate or incomplete, and the right to ask for their deletion when they have been unlawfully stored (Article 41(5) of SIS II Regulation and 58(5) of SIS II Decision).

Under the Schengen legal framework only the State which issues an alert in the SIS II 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.

Remedies: the right to complain to the data protection authority or initiate a judicial proceeding

Articles 43 of SIS II Regulation and 59 of SIS II Decision provide for the remedies accessible to individuals when their request has not been satisfied. Any person may bring an action before the courts or the authority competent under 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, national data protection authorities should cooperate with each other to guarantee the rights of the data subjects.

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