Data protection and the Schengen Information System

Republika Hrvatska
Ministarstvo unutarnjih poslova

What is the Schengen Information System?

The Schengen Information System is a common information system allowing the competent authorities in the Schengen Member States to cooperate by exchanging information. It is also an essential tool for the application of the provisions of the Schengen acquis. It was established to help maintain internal security within the Schengen States in the absence of internal border controls.

The Schengen Information System constitutes a compensatory measure contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between police authorities and judicial authorities in criminal matters.

It is a large-scale information system that enables police, judicial and other authorities with right of access to enter and consult alerts on missing persons, on persons or objects related to criminal offences and on non-EU nationals who are not allowed to enter or stay in the Schengen area. The newest version of the second generation Schengen Information System (SIS II) came into operation on 9 April 2013.

Depending on the type of alert, the SIS II is regulated either by the 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 (SIS II) 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 (SIS II).

What type of data does the SIS II contain?

The SIS II contains two categories of data which are supplied by each of the Member States: data on objects or persons in relation to whom an alert has been issued.

When the alert concerns a person, the information must always include the first and last name 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 the SIS II and the type of offence.

The SIS II contains the following alerts:

- alerts issued in respect of third-country nationals for the purpose of refusing entry and stay,
- alerts in respect of persons wanted for arrest for surrender or extradition purposes,
- alerts on missing persons,
- alerts on persons sought to assist with a judicial procedure,
- alerts on persons and objects for discreet checks or specific checks and
- alerts on objects for seizure or use as evidence in criminal proceedings.

What rights does a person have regarding data processed in the SIS II?

All individuals whose data are processed in the SIS II are granted specific rights by the SIS II Regulation and the SIS II Decision. These rights can be exercised in any country that operates the SIS II, regardless of the Member State that issued the alert.

Any person is entitled to request access to data related to them and entered in the SIS II, correction of inaccurate data and deletion of unlawfully stored data. Also, 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.

Right of access

Any person has the right to access data related to them and entered in the SIS II. The rules on access are exercised in accordance with the national law of the Member State concerned. Access may only be refused when this is indispensable for the performance of a lawful task in connection with an alert and for the protection of the rights and freedoms of other people.

The individual concerned 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.

Right of correction of inaccurate data and deletion of unlawfully stored data

Any person has the right to have factually inaccurate data relating to him corrected or unlawfully stored data relating to him deleted.

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.

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.

How to exercise right of access, correction of inaccurate data and deletion of unlawfully stored data in the SIS II in the Republic of Croatia?

Once the Council adopts a decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia, the individuals will be entitled to request access to data related to them and entered in the SIS II, correction of inaccurate data and deletion of unlawfully stored data. The individuals can exercise their rights via the submission of written request to the address of the Ministry of the Interior: Ulica grada Vukovara 33, 10 000 Zagreb.

Requests can also be submitted in person, orally, for the record with the Ministry of the Interior or in accordance with the procedure set in the Electronic Document Act and the Electronic Signature Act. Requests should be signed personally by the applicant or his legal representative. The procedure is free of charge.

The applicant must state his information (first and last name, personal identification number (if any), place of residence, place and date of birth and nationality). The request must be accompanied by a photocopy of a document proving the identity of the data subject – i.e. a national identity card or passport. In order to facilitate the exercise of data subject rights, the forms for access, correction and deletion of data from the SIS II are available on the MoI website. The data subject can be represented by a legal representative. The request should provide evidence of legal authorisation to represent the applicant.

Any questions regarding the exercise of data subject rights can be directed to the **data protection officer.** A person who considers that any of his/her rights have been violated may submit a request to establish the violation of rights to the **Personal Data Protection Agency.**