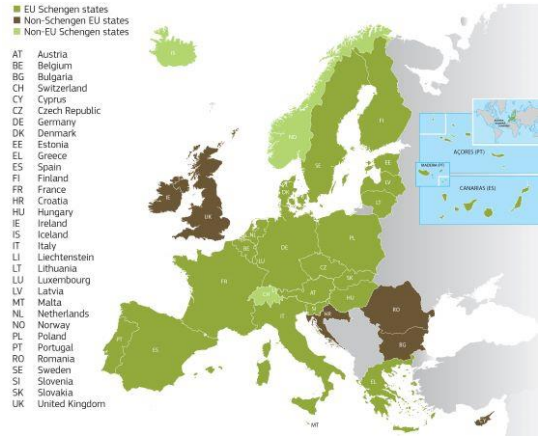
Schengen Information System

The Schengen Area

The free movement of persons is a fundamental right guaranteed by the EU to its citizens. It entitles every EU citizen to travel, work and live in any EU country without special formalities. Schengen cooperation enhances this freedom by enabling citizens to cross internal borders without being subjected to border checks. The border-free Schengen Area guarantees free movement to more than 400 million EU citizens, as well as to many non-EU nationals, businessmen, tourists or other persons legally present on the EU territory.

Today, the Schengen Area encompasses most EU States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. However, Bulgaria and Romania are currently in the process of joining the Schengen Area. Of non-EU States, Iceland, Norway, Switzerland and Liechtenstein have joined the Schengen Area.



The Schengen provisions abolish checks at the Union's internal borders, while tightening controls at the external borders, in accordance with a single set of rules.

What is the Schengen Information System?

The Schengen Information System (SIS) is the most widely used and largest information sharing system for security and border management in Europe. SIS enables competent national authorities such as the police and border guards, to enter and consult alerts on persons or objects. SIS is in operation in 30 European countries, including 26 EU Member States (only Ireland and Cyprus are not yet connected to SIS) and 4 Schengen Associated Countries (Switzerland, Norway, Liechtenstein and Iceland).

EU Member States with special arrangements:

- **Bulgaria**, **Romania** and **Croatia** are not yet part of the area without internal border checks (the 'Schengen area'). However, since August 2018, Bulgaria and Romania started using fully SIS. A Council Decision is still required for the lifting of checks at the internal borders of these two Member States. In the case of Croatia, there are still some restrictions regarding its use of Schengen-wide SIS alerts for the purposes of refusing entry into or stay in the Schengen area. Those restrictions will be lifted as soon as Croatia has become a part of the area without internal border checks.
- The **United Kingdom** operates SIS but, as it has chosen not to join the Schengen area, it cannot issue or access Schengen-wide alerts for refusing entry and stay into the Schengen area.

- **Ireland** and **Cyprus** are not yet connected to SIS. Ireland is carrying out preparatory activities to connect to SIS, but, as is the case for the UK, it will not be able to issue or access Schengen-wide alerts for refusing entry or stay. Cyprus has a temporary derogation from joining the Schengen area and is not yet connected to SIS.

An SIS alert does not only contain information about a particular person or object but also instructions for the authorities on what to do when the person or object has been found. The national SIRENE Bureaux located in each participating country serve as single points of contact for the exchange of supplementary information and coordination of activities related to SIS alerts.

On 9th April 2013 a more up-to-date system, called SIS II offering additional functionalities entered into operation.

A designated authority in each participating country has the responsibility for the operation of its section of the SIS. The N-SIS II Office (Ministry of Interior, Deputy State Secretariat for Data Registers, Department for Schengen Matters and Users Management), oversees the data processing activities, and must ensure that such data is limited to one of the SIS's defined purposes, such as border control, national security or law enforcement.

Should relevant information need to be transferred through the system, another authority acts as the central network exchange, SIRENE (Supplementary Information Request at National Entry) between the state and other cooperating countries. In Hungary SIRENE Bureau is part of the International Law Enforcement Cooperation Centre (Hungarian National Police Headquarters).

In June 2018, the co-legislators reached political agreement on the new SIS package. The new functionalities in SIS will be implemented in different stages, with a requirement for the work to be completed by 2021.

The changes will entail enhancements in the following areas:

- **Biometrics:** SIS will contain palm prints, fingerprints, facial images and DNA concerning, for example, missing persons to confirm their identity.
- **Counter-terrorism:** More information will be shared on persons and objects involved in terrorism-related activities, allowing the authorities of the Member States to better pursue and prevent serious crimes and terrorism.
- **Vulnerable persons:** Competent authorities will have the possibility of entering preventive alerts in the system to protect certain categories of vulnerable persons (missing persons, children at risk of abduction or potential victims of trafficking in human beings or gender-based violence).
- **Irregular migration:** Return decisions and entry bans will be part of the information shared in the system to enhance their effective enforcement.

- **Enhanced access for EU Agencies:** Europol will now have access to all alert categories in the SIS while the European Border and Coast Guard Agency operational teams will be able to access SIS for the purpose of carrying out their tasks in the hotspots.

Moreover, the introduction since March 2018 of an AFIS (Automated Fingerprint Identification System) in SIS, and the resulting possibility of making searches using fingerprints, makes it even more difficult for criminals to move unnoticed across Europe.

Who is affected and what types of data are stored in the SIS?

The type of personal data stored in the Schengen Information System is defined by the Regulation (EC) No 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, and is collected in accordance with the relevant laws of member states, which in Hungary are: Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System and the Government Decree No. 15/2013. (28/I) on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System.

Participating states may only collect data on:

- persons wanted for arrest in surrender or extradition procedure
- non-nationals for whom an alert has been issued for the purpose of refusing entry into the Schengen area
- missing persons, persons who need to be placed under protection
- witnesses or persons summoned to appear before judicial authorities in connection with a criminal matter, or those who are to be served with a criminal judgment or custodial sentence
- persons under discreet surveillance or specific checks
- documents, vehicles other objects specified in the legislation (firearms, boats, and identity documents), which are to be seized or used as evidence

It should be noted that personal data in the SIS may not pertain to one's racial background, political, religious or other beliefs, health status or sex life.

Functionalities of the SIS II:

- Enhanced alerts on persons and objects: persons, vehicles, firearms, issued documents, blank documents, bank notes.
- New categories of alerts: stolen aircrafts, boats, boat engines, containers, industrial equipment, securities and means of payment.
- Direct queries in the central system.
- Linking of alerts on persons, objects & vehicles (e.g.: alert on a person and a vehicle).

- Biometric data (fingerprints and a photograph).
- European Arrest Warrant attached directly to alert for persons wanted for arrest for surrender or extradition.
- Information on misused identity preventing the misidentification.
- Notations regarding specific objects may be made in the SIS, provided such items were forfeited or presented as evidence in criminal proceedings. Alerts may concern lost, stolen, misappropriated or invalidated

Who may use SIS data within participating states?

Each member state submits a list of competent institutions which are authorized to use data stored in the SIS to an EU Commission executive committee. The system can be accessed locally by a variety of approved authorities. Access is instant and direct.

Police, for example, may obtain SIS information for the purpose of protecting the legal order, national security or during the course of a criminal investigation.

Data that pertains to a refusal of entry into the Shengen zone, as well as specified types of lost, stolen or misappropriated goods may be accessed by:

- authorities responsible for issuing visas
- central authorities responsible for examining visa applications
- authorities responsible for issuing residence permits
- authorities responsible for the administration of legislation on aliens

Institutions in member states who are responsible for the issuance of vehicle registration certificates may also have access to data on stolen, misappropriated or invalidated vehicle registration certificates and license plates.

Your Data Protection Rights and the SIS

In order to understand your data protection rights vis-à-vis the SIS, it helps to understand the various institutions involved in its implementation.

The European Data Protection Supervisor shall check that the personal data processing activities in the eu-LISA are carried out lawfully and ensure that an audit of the eu-LISA's personal data processing activities is carried out in accordance with international audit standards at least every four years.

The National Supervisory Authorities and the European Data Protection Supervisor shall cooperate actively and ensure coordinated supervision of SIS II. They shall meet at least twice

a year. For the sake of transparency, a joint report of activities shall be sent to the European Parliament, the Council and eu-LISA every two years.

At the national level each signatory nation has a data protection authority that is tasked with the oversight of national data control issues. In Hungary, the independent office of the National Authority for Data Protection and Freedom of Information performs this function.

In accordance with EU and Hungarian laws, each person has the right to:

- access SIS-stored information related to the person
- request that inaccurate or false data is corrected
- request the removal of its unlawfully processed data
- turn to the courts or another competent authority to request the correction or removal of inaccurate data or petition for compensatory damages

In Hungary, anyone who is interested in knowing whether or not their data has been recorded in the SIS, or wishes to correct or have inaccurate data deleted should contact any government office, police station or any Hungarian Embassy or Consulate and fill in a request for information form which is transferred to the SIRENE Bureau of the Hungarian National Police Headquarters:

SIRENE Bureau

Address: 1139 Budapest, Teve u. 4-6.
Tel. : 443-5861
Fax : 443-5815
E-mail : nebek@nebek.police.hu

Form for requesting information on the basis of Art. 26 of the Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System

The SIRENE Bureau has the right to refuse requests but is obliged to inform the person about the fact of and the reason for denial. Should you find that the SIRENE Bureau is not adequately responsive to your request, you then may turn to the Hungarian National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information
Postal address: 1530 Budapest, Pf.: 5.
Office address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Tel: +36 1 391-1400
Fax: +36 1 391-1410
Email: ugyfelszolgalat@naih.hu
Web: http://naih.hu