Schengen Information System (SIS)

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 Cyprus and Ireland. On 31 March, 2024 Bulgaria and Romania became the newest Schengen members: the Schengen rules apply in both Member States including the issuing of Schengen visas and lifted controls at internal air and sea borders (checks at internal land borders between Bulgaria, Romania and the other Schengen countries have not yet been lifted). Additionally, non-EU States Iceland, Norway, Switzerland and Liechtenstein have joined the Schengen Area. In addition, the Schengen evaluation process to assess the readiness to join the Schengen area is ongoing for Cyprus. The Schengen Information System in Cyprus has been already put into operation since July 2023.

The Schengen provisions abolish checks at the Union's internal borders, while tightening controls at the external borders applicable to those who enter the Schengen area for a short period of time (up to 90 days). The Schengen area relies on common rules covering in particular the crossing the EU external borders, harmonisation of the conditions of entry and of the rules on short stay visas, cross-border police cooperation and stronger judicial cooperation as well as establishing the Schengen Information System (SIS).

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. As there are no internal borders between Schengen countries in Europe, SIS compensates for border controls and is the most successful cooperation tool for border, immigration, police, customs and judicial authorities in the EU and the Schengen associated countries. Competent national authorities, such as the police and border guards, are able to enter and consult alerts on people and objects in one common database.

Technically, SIS consists of three components: a central system (C.SIS), national SIS systems in all the countries using SIS (N.SIS) and a network between the systems.

Each country that uses SIS is responsible for setting up, operating and maintaining its national system and structures. The European Commission is responsible for general supervision, evaluating the system, and adopting implementing and delegated acts on how the SIS and SIRENE work. The EU Agency for large-scale IT systems (eu-LISA) is responsible for the operational management of the central system and the network.

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.

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).

Since 1995, the system has helped Europe preserve its security in the absence of internal border checks. Since the creation of its first version in 1995, the SIS system has been continuously developed and expanded in order to be able to meet the demands of the entry of new countries and to have new functions. In 2013, the second generation of SIS (SIS II) was rolled out, with additional functionalities and a new technical platform, such as the possibility of adding fingerprints and photographs to alerts.

In March 2023, **SIS was renewed** with new alerts, upgraded data and enhanced functionalities. New categories of alerts and more data are shared through SIS, ensuring that more complete and more reliable information is available to the authorities in countries that use SIS.

What types of alerts and data are stored in the SIS?

A SIS alert contains information about a particular person or object together with instructions for the authorities on what to do when the person or object has been found. SIS only contains alerts on people or objects in pre-determined alert categories.

- From March 2023, new categories of alerts and more data are shared through SIS, ensuring that more complete and more reliable information is available to the authorities in countries that use SIS: **Return decisions**: alerts in respect of third-country nationals subject to return decisions issued by the Schengen countries.
- **Refusal of entry or stay**: alerts covering third-country nationals who are not entitled to enter into or stay in the Schengen Area.
- **Persons wanted for arrest**: alerts for people for whom a European Arrest Warrant or Extradition Request (Switzerland and Liechtenstein) has been issued.
- **Missing persons**: alerts to find missing persons, including children, and to place them under protection if lawful and necessary.
- **Children at risk of being abducted by their own parents, relatives or guardians**: alerts to prevent such children from being abducted or going missing
- **Vulnerable persons whose travel must be prevented:** alerts to protect vulnerable people (adults or children) from being taken unlawfully abroad or to prevent them from travelling without the necessary authorisations.
- **Persons sought to assist with a judicial procedure**: alerts to find out the place of residence or domicile of people sought to assist with criminal judicial procedures (for example witnesses).

- **Persons and objects for discreet, inquiry or specific checks**: alerts to obtain information on people or related objects for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security.
- **Unknown wanted persons**: alerts containing only finger-marks and palm marks belonging to a perpetrator of an offence discovered at the scenes of terrorist offences or other serious crimes under investigation. They are issued for the purposes of identifying the perpetrator under national law.
- **Objects for seizure or use as evidence in criminal procedures**: alerts on objects (for example vehicles, travel documents, number plates and industrial equipment) being sought for seizure or use as evidence in criminal proceedings. Alerts on travel documents may also be issued specifically for preventing travel by the person who holds them.

The quality, accuracy and completeness of the data elements enabling identification are key to the success of SIS. For alerts on people, the minimum data set is:

- name
- year of birth
- a reference to the decision giving rise to the alert
- the action to be taken

When available, photographs and fingerprints must be added in order to facilitate identification and to avoid misidentification. The system also offers the possibility of adding links between alerts (for example, between an alert on a person and a vehicle).

Since 2013, SIS has been able to store fingerprints which may be used to confirm the identity of a person located by other means. The introduction of an **AFIS (Automated Fingerprint Identification System)** in March 2018 also allows people to be identified using just their fingerprints. As of March 2023, SIS also stores palm prints, finger-marks and palm marks. These are used for biometric searches and for the confirmation of identities. From March 2023, SIS also stores DNA profiles of people reported missing or of their parents, grandparents or siblings for the purpose of confirming identity.

Who has access to the data in SIS?

SIS is a highly secure and protected database that is exclusively accessible to authorised users within competent authorities who are responsible for border control, police and customs checks the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the enforcement of criminal penalties, examining visa applications and taking decisions relating to those applications etc.

The new SIS also gives wider access to other national authorities, such as competent national authorities who are responsible for issuing residents permits and long-stay visas as well as naturalisation, issuing registration certificates for vehicles, issuing registration certificates or ensuring traffic management for boats, including boat engines, and aircraft, including aircraft engines, issuing registration certificates for firearms, etc.

Several European Union agencies will have wider access to the SIS system. Members of Europol, Eurojust and Frontex teams have access to all data categories of the SIS to the extent necessary to carry out their tasks.

A list of competent national authorities with access to SIS is published annually in the Official Journal of the European Union.

Data Subject's Rights and the SIS

SIS has strict requirements on data quality and data protection. The national data protection authorities supervise the application of the data protection rules in their respective countries, while the European Data Protection Supervisor monitors how the data protection rules are being applied in the central system managed by eu-LISA. Both levels work together to ensure coordinated end-to-end supervision.

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

You can exercise any of the above mentioned rights in any of the countries using SIS. Questions regarding the legality of collected data are reviewed according to the laws of the member state where the complaint has been brought. If the data concerned was recorded by another member state, the two states will closely collaborate to consider any legal issues. The national procedures and contact points for access requests for each country can be found in the *Guide for exercising the right of access* available on the website of the European Data Protection Supervisor (https://www.edps.europa.eu/data-protection/our-work/publications/scg-documents/guide-exercising-right-access_en).

In Hungary, anyone can request information of data stored on them in the SIS and have inaccurate data rectified or have unlawfully stored data erased. The request shall be submitted by the data subject or by their authorized lawyer in person at any Hungarian government office, any Hungarian police station or any Hungarian Consulate. The request is transferred to the SIRENE Bureau of the Hungarian National Police Headquarters'.

Your request shall include the following data:

1. Personal data of the applicant:

1.1. Family name(s) and surname(s)

1.2. Family name(s) and surname(s) at birth

1.3. Place and date of birth

1.4. Sex

1.5. Nationality

1.6. Travel document number (ID number)

1.7. Address (only one is required)

1.8. Mailing address (only one is required)

1.9. Phone number (optional)

1.10. Other contact details (e-mail, fax) (optional)

2. Applicant's other communications

Contact details of the Hungarian Consulates:

https://konzinfo.mfa.gov.hu/en/embassies#hungarian-embassies-abroad

SIRENE Bureau

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

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 as well as about the possibility of legal remedy provided by the Privacy Act. 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 to initiate a revision procedure for the protection of your personal data.

If you decide so instead or beside these actions you may bring a lawsuit and ask the civil law court to make the data controller reimburse your financial loss related to unlawful data processing.