What is the Schengen Information System?

Travel in much of Europe today most often means little more than a short ID and background check at the initial border crossing. Visitors and goods are then generally free to move throughout the Schengen area without the hassle of further border controls. Such border-free travel would not be possible, however, without access to a Schengen-wide system of data exchange, as well as an agreed-upon set of procedures regulating entry. The Schengen Information System (SIS), therefore, is a database created to ensure that participating countries have access to relevant information on individuals and property of interest.

A designated authority in each participating country has the responsibility for the operation of its section of the SIS. The authority, or N-SIS (the Central Office for Administrative and Electronic Public Services – COAEPS), oversees the collection and dissemination of relevant information, 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. Institutions in Brussels and Strasbourg work to ensure that data is consistent throughout the system and provide technical support to all participating states.

Which countries participate in the SIS?

Signatory states to the Convention Implementing the Schengen Agreement (CISA) may share information through the SIS. Currently, most countries in Europe take part in the system. The Republic of Ireland and the United Kingdom participate by virtue of the *Schengen Acquis*, which has now been incorporated into European legislation. Although these two countries remain outside of the Schengen zone, they may only take advantage of SIS as a law enforcement resource. Non-EU countries Iceland, Norway, Liechtenstein and Switzerland are full participants in the SIS, as they have lifted border controls between themselves and other Schengen zone states. Romania and Bulgaria are currently in negotiations to join the Shengen area.

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 Schengen Convention, and is collected in accordance with the relevant laws of member states.

Member states may only collect personal 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

The personal data collected is limited to:

- surname and forenames, any possible aliases, middle initial
- objective and physical characteristics not subject to change
- date and place of birth
- sex
- nationality
- whether the person concerned is armed
- whether the person concerned is violent
- reason for the alert
- action to be taken should person be encountered

Notations regarding specific objects may be made in the SIS, provided such items were forfeited or presented as evidence in criminal proceedings.

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.

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, examining

visa applications, issuing residence permits and the administration of legislation on aliens.

For a more exhaustive list, interested parties should contact their national SIRENE office.

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 Joint Supervisory Authority (JSA) is an independent body based in Brussels, whose main role is to ensure that the operation of the SIS is in full compliance with data protection laws and citizens' rights. The JSA provides multi-faceted support to SIS users, including addressing issues of application or interpretation. It may deliver opinions and provide technical assistance at the governmental level.

Each signatory nation has a data protection authority that is tasked with the oversight of national data control issues. As of 1 January 2012, the independent office of the National Authority for Data Protection and Freedom of Information performs this function in Hungary.

In agreement 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 or removed
- turn to the courts or another competent authority to request the correction or removal of inaccurate data or petition for compensatory damages

Relief for infractions of any of the above may be pursued in each Schengen member state. 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.

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 in person any 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.

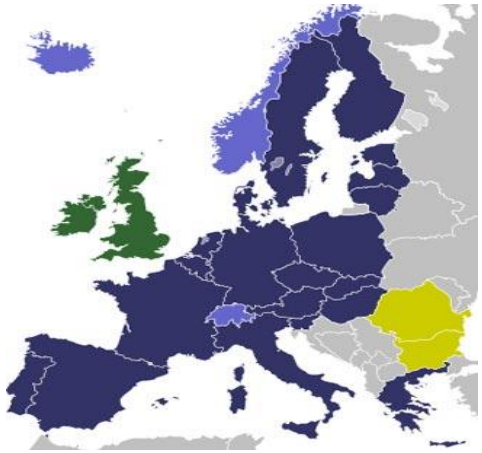
The Bureau has the right to refuse requests but is obliged to inform the person about the fact of and the reason for denial. Should you find that the SIRENE Bureau is not adequately responsive to your request, you then may turn to the Hungarian National Authority for Data Protection and Freedom of Information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

Nemzeti Adatvédelmi és Információszabadság Hatóság
Postal: 1534 Budapest, Pf.: 834
Office: 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

National Authority for Data Protection and Freedom of Information

INTRODUCTION TO

THE SCHENGEN INFORMATION SYSTEM



Courtesy of the National Authority for Data Protection and Freedom of Information, Hungary

2012