General Data Protection Regulation – information to be provided to visa applicants concerning the personal data provided upon application

Information on the processing of your personal data:

The collection of your personal data required by this application form, the taking of your photograph and the taking of your fingerprints are mandatory for the examination of your visa application. Failure to provide such data will result in the application being inadmissible.

The authorities responsible for processing the data in Hungary are: Ministry of Foreign Affairs and Trade, H-1027 Budapest, Bem rkp. 47., https://www.kormany.hu/en/ministry-of-foreign-affairs-and-trade/missions, E-mail: konz@mfa.gov.hu; National Directorate-General for Aliens Policing, H-1117 Budapest, Budafoki út 60, http://www.bevandorlas.hu/, E-mail: migracio@bah.b-m.hu

Contact details of the data protection officers: Ministry of Foreign Affairs and Trade, H-1027 Budapest, Bem rkp. 47., DPO: Szilvia Molnár-Friedrich dr. , E-mail: kozadat@mfa.gov.hu; SzMolnar-Friedrich@mfa.gov.hu, Tel.: +36-1-458-1597; National Directorate-General for Aliens Policing, H-1117 Budapest, Budafoki út 60, DPO: Norbert Andó, E-mail: adatvedelem@bah.b-m.hu, Tel.: +36-1-463-9100

The legal basis for the collection and processing of your personal data is set out in Regulation (EC) No 767/2008 (VIS Regulation), Regulation (EC) No 810/2009 (Visa Code) and Council Decision 2008/633/JHA.

The data will be shared with the relevant authorities of the Member States and processed by those authorities for the purposes of a decision on your visa application.

The data and data concerning the decision taken on your application or a decision whether to annul, revoke or extend a visa issued will be entered into, and stored in the Visa Information System (VIS) for a maximum period of five years, during which it will be accessible to the visa authorities and the authorities competent for carrying out checks on visas at external borders and within the Member States, immigration and asylum authorities in the Member States for the purposes of verifying whether the conditions for the legal entry into, stay and residence on the territory of the Member States are fulfilled, of identifying persons who do not or who no longer fulfil these conditions, of examining an asylum application and of determining responsibility for such examination. Under certain conditions the data will be also available to designated authorities of the Member States and to Europol for the purpose of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

Your personal data might also be transferred to third countries or international organisations for the purpose of proving the identity of third-country nationals, including for the purpose of return. Such transfer may only take place under certain conditions[1]. You can contact the

[1] Article 31 of Regulation (EC) No 767/2008 (VIS Regulation)

authority responsible for processing the data (see contact details above) to obtain further information on these conditions and how they are met in your specific case.

Under the General Data Protection Regulation[2] and the VIS Regulation[3], you are entitled to obtain access to your personal data, including a copy of it, as well as the identity of the Member State which transmitted it to the VIS. You also have the right that your personal data which is inaccurate or incomplete be corrected or completed, that the processing of your personal data be restricted under certain conditions, and that your personal data processed unlawfully be erased.

You may address your request for access, rectification, restriction or erasure directly to the authority responsible for processing the data (see contact details above). Further details on how you may exercise these rights, including the related remedies according to the national law of the State concerned, are available on its website and can be provided upon request.

You may also address your request to any other Member State. The list of competent authorities and their contact details is available at: https://edpb.europa.eu/about-edpb/board/members_en

You are also entitled to lodge at any time a complaint with the national data protection authority of the Member State of the alleged infringement, or of any other Member State, if you consider that your data have been unlawfully processed. The data protection authority of Hungary is: Hungarian National Authority for Data Protection and Freedom of Information, H-1125 Budapest, Szilágyi Erzsébet fasor 22/C; E-mail: ugyfelszolgalat@naih.hu, Website: http://www.naih.hu/

Please refer to the competent visa authority for information on the processing of other personal data that may be necessary for the examination of your application.

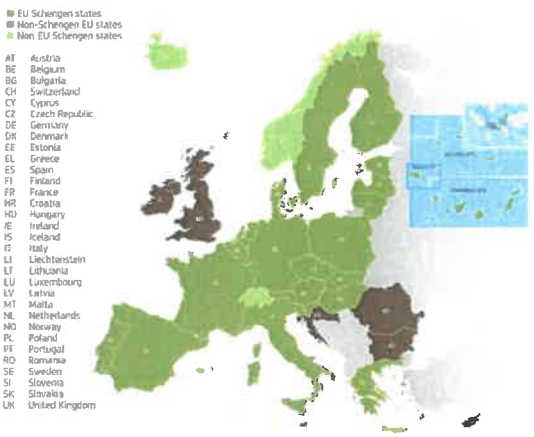
[2] Articles 15 to 19 of Regulation (EU) 2016/679 (General Data Protection Regulation)
[3] Article 38 of Regulation (EC) No 767/2008 (VIS Regulation)

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

Visa Information System

The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

Data is fed into the VIS by national authorities. The authorities with access to VIS must ensure that its use is limited to that which is necessary, appropriate and proportionate for carrying out their tasks. Furthermore, they must ensure that in using VIS, the visa applicants and holders are not discriminated against and that their human dignity and integrity are respected.

What kind of data is stored in the VIS database?

10 fingerprints and a digital photograph are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database.

10-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

At the Schengen Area's external borders, the visa holder's finger scans may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused - it will merely lead to further checks on the traveller's identity.

In accordance with Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) data is stored in the VIS database if:

- it is entered immediately upon application (Art.9)

- stored once a visa is issued (Art.10);
- the visa request examination process is discontinued (Art.11);
- the visa was refused (Art.12);
- the visa was revoked (Art.13);
- the visa is extended (Art.14).

Data stored into the database concerns the identity of the authority examining the application, elements (like date, type of the visa) on the application process itself, the name of the applicant, the purpose of the travel, the length of the stay, a photography and a fingerprint.

Data is kept in the VIS system for up to 5 years, but if the data subject obtains a Member State's citizenship, his record must be erased immediately.

Which countries use VIS and who operates it?

As a Schengen instrument, VIS applies to all Schengen States (Denmark has decided to implement it). The EU Agency for large-scale IT systems, eu-LISA, is responsible for the operational management of VIS.

Who can access VIS?

Competent visa authorities may consult the VIS for the purpose of examining applications and decisions related thereto.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories.

Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application.

In specific cases, national authorities and Europol may request access to data entered into the VIS for the purposes of preventing, detecting and investigating terrorist and criminal offences. (see Council Decision 2008/633/JHA of 23 June 2008 for further information).

What are the data subject's rights?

Visa applicants must be given appropriate information from the national authorities that handle their request for a visa. This information should cover the nature of the data that is collected, the purpose of the collection, the period of retention of the data, which information is compulsory for the visa application process and which one isn't, and who can be granted access to this data.

Data subjects have a right to access their data, and ask for correction of false information as well as request deletion of unlawfully collected data. Each State being responsible for the data it feeds into the VIS, data subjects who are victims of unlawful VIS data processing may sue for compensation.

National data protection authorities and the European Data Protection Supervisor (EDPS) cooperate to ensure the compliance of the VIS database with data protection rules.

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

- access VIS-stored information related to the person
- request the correction of inaccurate or false data
- 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

WHEN ABROAD

The request has to be lodged abroad to the authority that carries/carried on the procedure. More information can be found at the http://konzuliszolgalat.kormany.hu/en webpage.

WHEN IN HUNGARY

The request has to be lodged in Hungary to the National Directorate-General for Aliens Policing

H-1117 Budapest, Budafoki út 60,

http://www.bevandorlas.hu/

E-mail: migracio@bah.b-m.hu

The authority 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 authority 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