



Schengen Information System



What is the Schengen Information System?

The Schengen Information System¹ (SIS) is a collaborative electronic law enforcement search and information system established by the Schengen States as one of the most important compensatory measures for the abolition of internal border checks and the fight against cross-border crime in Europe.

SIS contains alerts on persons and objects. Alerts on persons may be recorded in SIS for the following reasons:

- A person is wanted for arrest or
- sought to assist with a judicial procedure.
- A person is missing.
- A vulnerable person or minor has to be prevented from travelling for their own protection.
- A person is subject of discreet checks.
- A third-country national² is subject of a return decision or a refusal of entry or stay in the Schengen Area.
- An unknown wanted person is sought as a perpetrator of an offence based on fingerprints.

Alerts on objects are issued for sought vehicles, firearms, documents and banknotes for seizure or use as evidence in criminal proceedings.

Currently, SIS has 30 users:

Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden as well as the associated members Iceland, Liechtenstein, Norway and Switzerland. Cyprus is a Member State of the EU, but does not participate in the Schengen Area. The microstates Monaco, San Marino and Vatican City are de facto part of the Schengen Area, as all of their borders are with the Schengen States France and Italy, and no border controls are in place.

¹ Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

² Third-country nationals are individuals who are neither EU citizens, nor EEA citizens nor Swiss nationals.

Which personal data is stored in SIS?

The categories of data that are eligible to be processed in SIS particularly include³: surnames and forenames; names at birth; previously used names; aliases; place and date of birth; sex; specific physical characteristics not subject to change; photographs; fingerprints; nationality; whether the person concerned is armed, violent or has escaped; reason for the alert; authority issuing the alert; a reference to the decision giving rise to the alert; the type of criminal offence underlying the alert; action to be taken; numbers of identity papers and date of issue.

What rights do you have regarding data stored in SIS?

Each person has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed in SIS. This right is based on Art. 53, para. 1 of Regulation (EU) 2018/1861⁴, Art. 67, para. 1 of Regulation (EU) 2018/1862⁵ and the national law of the Member State on whose territory this right is exercised. The relevant legal provisions in Austria are section 44 of the Austrian Data Protection Act (DSG)⁶, Art. 15 through 17 of the General Data Protection Regulation (GDPR), as well as Art. 14 and Art. 16, para. 1 and 2 of Directive (EU) 2016/680⁷. The application can be filed using an electronic signature.

As a safeguard against misuse, you are required to sufficiently prove your identity to the data controller (any former names, date of birth, place/country of birth, parents' forenames, nationality, additional home addresses) if you request access to any personal data concerning you that may be stored in SIS. In accordance with section 42, para. 7 of the DSG, the controller may demand

³ See Art. 20 of the Regulation (EU) 2018/1862.

⁴ Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

⁵ Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

⁶ Austrian Data Protection Act (DSG), Federal Law Gazette 2021/148, as amended and updated from time to time.

⁷ Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

additional necessary information in order to verify the identity of the person who has filed an application pursuant to sections 44 and 45 of the DSG. The request for access must be in writing. Telephone requests cannot be answered for legal reasons.

What does this right of access mean?

Each person not only has the right to request access to their personal data that has been entered in SIS, but also – in accordance with Art. 53 of Regulation (EU) 2018/1861 in connection with sections 44 and 45 of the Austrian Data Protection Act (DSG) as well as Art. 16 and 17 of the General Data Protection Regulation – has the right to have inaccurate personal data corrected or unlawfully stored personal data deleted. If the operation of SIS infringes on a person's rights, the respective member state is liable – to the extent defined by its national law – for any damage suffered. In Austria, the relevant legal provisions are Art. 82 of the of the General Data Protection Regulation in connection with section 29 of the DSG.

Who is responsible for SIS in Austria?

In Austria, the Federal Ministry of the Interior (BMI) is responsible for operating the national part of SIS. Due to this responsibility, i.e. as a controller, the BMI is also required to provide information pursuant to section 44 of the DSG. Thus, a request for information has to be submitted to the following BMI address:

Bundesministerium für Inneres
Bundeskriminalamt, Sirene Österreich
Josef-Holaubek-Platz 1
A-1090 Vienna
Austria

For details on how to obtain information on data protection matters from the BMI and Austria's law enforcement agencies, please visit the website of the BMI (www.bmi.gv.at).

Who supervises data processing in SIS?

Each Member State shall establish a National Supervisory Authority to monitor the lawfulness of the processing of SIS personal data on its territory independently. In Austria, the Data Protection Authority (DSB) has been designated as National Supervisory Authority. Anyone who feels that their rights were violated or that controllers or processors violated their duties can file a complaint with or send a message to the DSB.

For details on this process, please consult the website of the DSB at www.dsb.gv.at. The DSB provides no information on data stored in SIS; rather, the DSB is in a position to check whether provided information or the denial of information is lawful.

Another authority supervising compliance with data privacy is the European Data Protection Supervisor⁸ (www.edps.europa.eu). Within the scope of their respective jurisdictions, the National Supervisory Authority and the European Data Protection Supervisor actively collaborate to ensure coordinated monitoring of SIS.

Legal notice:

Media owner:

Federal Ministry of the Interior of Austria (Bundesministerium für Inneres (BMI), Criminal Intelligence Service Austria (Bundeskriminalamt), II/BK/2.3),
Josef-Holaubek-Platz 1, 1090 Vienna;

Layout:

Referat I/C/10/a (Strategische Kommunikation und Kreation);

Printed by:

BMI/Digital Print Center;

Address: 1010 Vienna, Herrengasse 7, Austria