What is the Schengen Information System (SIS)?

The SIS is a Europe-wide electronic person and object search facility system jointly operated by the Schengen countries. It contains information on persons wanted by police and judicial authorities, persons subject to non-admission, missing persons, and stolen objects (such as cars or firearms). The SIS is a pivotal facility for cooperation between police and judicial authorities.

As a result of the Schengen Agreement, systematic controls at the borders between the Schengen countries are being eliminated in order to facilitate travelling. By improving cross-border police cooperation at the same time, security and order in the Schengen Area will be ensured and improved.

On April 9, 2013, the SIS II has replaced the previous SIS1forALL. The SIS II contains over 45 million alerts. The largest number relates to stolen or lost documents (over 39 million) and stolen vehicles (about 5 million). The number of alerts for tracing persons is currently about 1.2 million. With the new SIS II, the capacity of possible alerts has been increased to 70 million. ¹

Schengen countries²

Associated Members (non-EU):
- Iceland
- Norway
- Switzerland
- Liechtenstein

EU, SIS access for law enforcement purposes:
- Romania
- Bulgaria
- United Kingdom

EU, but currently no SIS access
- Ireland
- Croatia
- Cyprus

---

¹ Status: 9 April 2013.
² Status: May 2015.
What data relating to a specific person can be stored in the SIS?

The SIS contains alerts concerning persons and objects. These are intended to enable the competent authorities to identify a specific person or object and take the necessary measures.

The alerts in the SIS concern:

- citizens of third (non-Schengen) countries who are refused admission or stay in the Schengen Area;
- persons wanted for arrest for the purpose of surrender or extradition;
- missing persons (who might have to be taken into custody);
- persons wanted for participation in court proceedings;
- persons or objects for discreet or specific check;
- issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated;
- documents, licence plates, securities and means of payment, etc.;
- objects for the purpose of seizure or use as evidence in criminal proceedings.

No more than the following personal data may be stored in the SIS on any specific person:³

- last name(s), forename(s), maiden name(s), and alias(es);
- special permanent physical characteristics;
- date and place of birth;
- sex;
- photographs;
- fingerprints;
- nationality or nationalities;
- 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;
- action to be taken;
- link(s) to other alerts issued in SIS II;
- the type of offence.

³ Article 10 N-SIS Ordinance.
Which authorities may access the data of the SIS?

In Liechtenstein, the following authorities have access to the SIS data to carry out their duties:

- the National Police (Landespolizei);\(^4\)
- the Migration and Passport Office (Ausländer- und Passamt), limited to accessing data in connection with alerts on citizens of third countries for refusal of admission and alerts concerning lost blank documents and identification documents.\(^5\)

Die National Police may provide information to the following other authorities on alerts in the SIS concerning persons or objects:\(^6\)

- the Swiss Federal Customs Administration (Eidgenössische Zollverwaltung), which is the competent customs authority in Liechtenstein due to the Customs Treaty;
- the Driver and Vehicle Licensing Office (Motorfahrzeugkontrolle) to check if a vehicle presented to it has been stolen or has been lost otherwise, or if it is wanted as evidence in criminal proceedings.

What rights does a person have concerning the data processed in the SIS?

A person concerned has the following rights:

- right of access concerning the data in the SIS relating to him or her;\(^7\)
- right of rectification of incorrect data and right of deletion of unlawfully stored data relating to him or her;\(^8\)
- right of complaint, to enforce a request for access, rectification, deletion, or damages submitted in a Schengen country;\(^9\)
- claim for damages in the event of unlawful data processing.\(^10\)

What is the right of access?

Everybody has the right to be informed as to whether data on him or her are being processed in the SIS, and if that is the case, to access that data.

In Liechtenstein, everybody may request information on whether data on him or her are being processed, and on the origin of that data. Such information may be limited or refused, in particular if this is required by prevailing public interests or by the internal or external security of the country, or if providing such information would endanger a criminal investigation or other investigation proceedings.

The request for information on data stored in the SIS may be submitted to the competent authority of any Schengen country.

---

\(^4\) Article 18 (1) N-SIS Ordinance.
\(^5\) Article 18 (2) N-SIS Ordinance.
\(^6\) Article 18 (3) N-SIS Ordinance.
\(^7\) Article 47 (1) and article 48 N-SIS Ordinance.
\(^8\) Article 47 (2) and article 48 N-SIS Ordinance.
\(^9\) Article 47 (3) and article 48 N-SIS Ordinance.
\(^10\) Article 50 N-SIS Ordinance in connection with article 14a Official Liability Act.
In **Liechtenstein**, such a request may be submitted in writing to the **National Police**. The requesting person must provide proof of his or her identity (copy of passport or identity card).

Address:

**Landespolizei des Fürstentums Liechtenstein**

Kommando
Postfach 684
Gewerbeweg 4
9490 Vaduz
Principality of Liechtenstein

The procedure for handling requests for access are subject to the national laws of the Schengen country where the request was submitted. In Liechtenstein, the request must generally be answered within 30 days, but no later than 60 days from the correct submission of the request.\(^\text{11}\)

**What is the right of rectification and deletion?**

Everybody has the right to **have rectified** any incorrect data stored in the SIS and relating to him or her and to have **deleted** any inadmissible or unlawfully obtained data.

The request for the rectification of incorrect data stored in the SIS may be submitted to the competent authority of any Schengen country.

In **Liechtenstein**, requests for rectification, deletion, and information must be submitted to the **National Police** (cf. above address).

The procedure for handling requests for rectification and deletion are subject to the national law of the Schengen country where the request was submitted. In Liechtenstein, the person concerned must be informed on the measures taken no later than 3 months after the correct submission of the request.\(^\text{12}\)

**Who to contact if the competent authority rejects or refuses the request for access, rectification, or deletion?**

In every Schengen country, there is an authority that handles complaints in connection with requests concerning the processing of data in the SIS.

In Liechtenstein, a **complaint (Beschwerde)** may be submitted to the **Data Protection Commission (Datenschutzkommission)** within 14 days from service of an order in which the National Police denies the claim for rectification or refuses the request for deletion and information. Decisions of the Data Protection Commission may in turn be appealed within 14 days by complaint to the **Administrative Court (Verwaltungsgerichtshof)**.\(^\text{13}\)

---

\(^{11}\) Article 47 (1) and article 48 N-SIS Ordinance.

\(^{12}\) Article 47 (2) and article 48 (5) N-SIS Ordinance.

\(^{13}\) Article 47 (3) N-SIS Ordinance.
Complaints must be submitted in writing and be addressed to the Data Protection Commission, for the attention of Chairwoman lic. iur. Mirjam Amann.

Address:
Datenschutzkommission (DSK)
Landstrasse 1
Postfach 1261
9490 Vaduz
Principality of Liechtenstein

What is the claim for damages?
If damage has occurred during the operation of the SIS and if such damage has been caused by the Principality of Liechtenstein as the country submitting the alert, the person who has suffered the damage may claim reimbursement under the following requirements:14

- damage has occurred;
- the authority has caused the damage by unlawful action
- due to official activity

(for example, as a result of the incorrect or unlawful processing of data).

If the injured person wants to assert his or her claim, he or she must ask the corresponding authority in writing to acknowledge the claim for reimbursement.15

Who supervises data processing in the SIS?
In every Schengen country, a national supervisory authority supervises the lawfulness of the processing of personal data in the SIS for the territory of the country in question as well as the transfer of such data from that territory.16

In Liechtenstein, it is the Data Protection Office (Datenschutzstelle) that supervises the processing of personal data in the national part of the SIS.

Address:
Datenschutzstelle (DSS) phone +423 236 60 90
Kirchstrasse 8
Postfach 684
9490 Vaduz
Principality of Liechtenstein
http://www.dss.llv.li

The Schengen Joint Supervisory Authority (JSA), consisted of representatives of the national supervisory authorities and was the supervisory authority for theSIS1forall, the previous system of the SIS II. The JSA oversaw the Schengen states whether the use of data in the SIS was lawful. With the introduction of SIS II on April 9, 2013, the legal basis for this institution has ceased to exist, at the same time a new basis for a new supervisory body has been created. The SIS Supervision Coordination Group (SIS SCG) monitors the use of the data in the SIS II. The legal basis is the SIS II Regulation (EC) No 1987/2006 of 20 December 2006)

14 Article 50 N-SIS Ordinance in connection with article 14a Official Liability Act.
15 Article 50 N-SIS Ordinance in connection with article 11 (2) Official Liability Act.
16 Article 114 Convention Implementing the Schengen Agreement.
and the SIS II Decision (2007/533/JHA of 12 June 2007). The SIS SCG holds meetings at least twice a year. The member states support each other in carrying out audits and inspections, clarify difficulties of interpretation or application of the legal basis, draw up harmonized proposals for joint solutions to common problems, promote awareness of data protection rights and trace difficulties in the exercise of independent supervision or the exercise of the rights of data subjects. Additionally, recommendations are finalized for the attention of the Member States and experiences are exchanged.

**Other useful links:**

**Schengen countries:**

- Swiss Federal Data Protection and Information Commissioner (*Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, EDÖB*): [http://www.edoeb.admin.ch](http://www.edoeb.admin.ch) (German, English, French)
- Austrian Data Protection Commission (Österreichische Datenschutzkommission, DSK): [https://www.dsb.gv.at](https://www.dsb.gv.at) (German, English)
- The European Data Protection Supervisor (EDPS) is an independent authority on a European level for the protection of privacy:

  **Duties:**

  - supervision of the processing of personal data by the administrative bodies of the EU;
  - counselling with regard to political measures and legal provisions affecting the protection of privacy;
  - cooperation with comparable authorities in order to ensure coherent data protection.

  [https://secure.edps.europa.eu/EDPSWEB](https://secure.edps.europa.eu/EDPSWEB) (EU languages)

Information as of October 2015