



«SCHENGEN» AND YOUR PERSONAL DATA

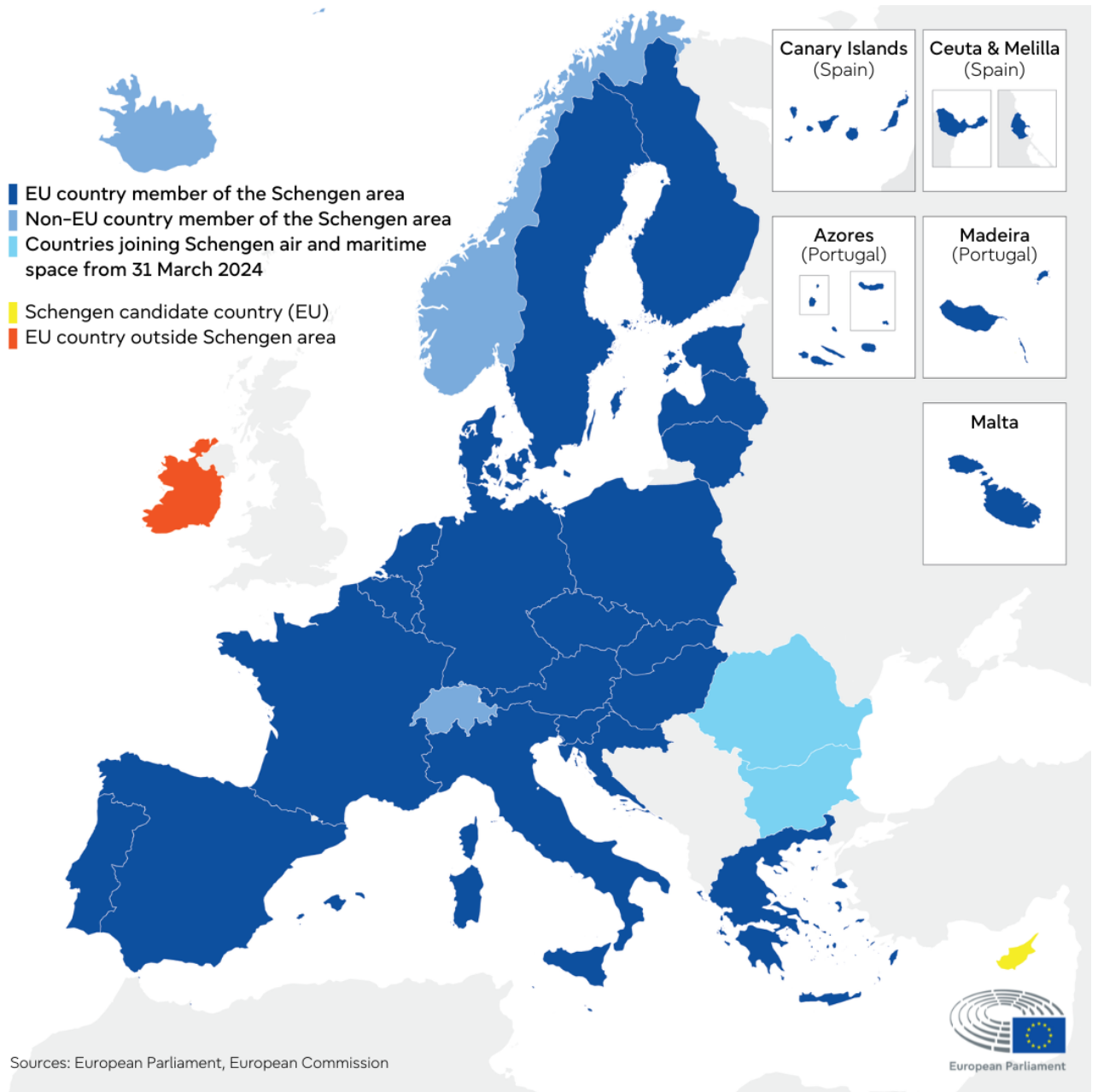
➤ What is the Schengen Information System (SIS)?

The SIS is a Europe-wide electronic **system for sharing information on persons and objects** operated jointly by the Schengen states. The SIS contains information on persons wanted by police and judicial authorities, persons subject to entry bans and missing persons, as well as on stolen objects (e.g. cars, weapons). It forms the centrepiece of Schengen's police and judicial cooperation. As a Schengen-associated country, **Switzerland** has access to the SIS.

Within the Schengen area, systematic checks on persons at internal borders were abolished, which has made travelling easier. At the same time, **cross-border police cooperation** between the Schengen states was **strengthened** thanks to the SIS.

Development of the SIS: After SIS II replaced SISone4all in April 2013, SIS II was expanded in March 2023 and is once again known as SIS. The latest SIS contains new alert categories, updated data and advanced functions. The enhanced information includes **biometric data** (photos, palm and fingerprints, palm and fingerprint traces and DNA records of missing persons). To **combat terrorism**, the member states have also been exchanging hits on SIS alerts in connection with terrorist offences with Europol since March 2021. **Vulnerable persons** (children, potential victims of terrorism, human trafficking, gender-based violence, armed conflicts or disputes) and information relating to **irregular migration** (return decisions, alerts for refusal of entry and stay) can also be entered in the SIS. The authorities authorised to access the SIS, such as the police, border guards or border control points at airports, carry out numerous SIS searches every day, for which they receive feedback in real time. In this way, these authorities contribute to security in Switzerland.

Member States: A total of 29 countries use the SIS on a daily basis. The majority of these are EU member states (Ireland does not participate) and the Schengen-associated countries (Switzerland, Liechtenstein, Norway, Iceland). Croatia has also been part of the Schengen area since 1 January 2023 and Romania and Bulgaria at the EU's internal air and sea borders as of 31 March 2024.



(Image from 12/01/2024, [Schengen: enlargement of Europe's border-free area | Topics | European Parliament \(europa.eu\)](#))

➤ **What personal data is stored in the SIS?**

The SIS only contains alerts for persons (and objects) that can be assigned to one of the following alert categories:



- third country nationals subject to refusal of entry or stay in the Schengen area or subject to return procedures
- wanted persons (by European arrest warrants or extradition request)
- missing persons
- children with an increased risk of abduction and vulnerable persons (including adults)
- persons sought to assist with a criminal judicial procedure (e.g. witness)
- persons subject to discreet, inquiry or specific checks (prosecution of criminal offences and prevention of threats to public or national security)
- unknown wanted persons for the purpose of identifying delinquent under national law
- objects for seizure / as evidence in criminal proceedings (e.g. vehicles, travel documents, licence plates, etc.).

The **minimum data set** for **person alerts** consists of:

- Name
- Year of birth
- Reference to the decision on which the alert is based
- Measure

Other data recorded in the SIS:

- Photos
- Finger and palm prints
- Finger and palm print traces
- DNA profiles of persons reported missing or their parents, grandparents, siblings
- Links between alerts

➤ Which authorities can access the SIS data?

Authorities under EU law (Article 34 para. 1, 2, 3 and Article 35 (EU) 2018/1861) - non-exhaustive list:

- national authorities responsible for the identification of third-country nationals
- national naturalisation authorities
- national judicial authorities
- Europol and Eurojust (restricted access)
- European Border and Coast Guard (Article 2 no. 8 and 9 (EU) 2016/1624)

Swiss authorities (Article 7 N-SIS):

- fedpol
- Office of the Attorney General



- Federal Office of Justice
- cantonal police and judicial authorities and the authorities responsible for enforcing expulsions
- Federal Office for Customs and Border Security (in particular Border Guard Corps, customs investigation and other customs offices)
- State Secretariat for Migration
- Swiss representations abroad (examination of visa application)
- Federal Intelligence Service (in particular agencies responsible for implementing the Intelligence Service Act)
- Cantonal and communal migration authorities
- Road traffic and shipping authorities
- Cantonal weapons offices

➤ What rights does a person have regarding the data processed about them in the SIS?

Rights of data subjects:

- Right of access
- Right to rectification
- Right to erasure
- Right to compensation

➤ What is the right of access?

The **right of access** is regulated in Article 25 of the Data Protection Act (DPA) and Article 14 of the Law Enforcement Directive (LED or Directive (EU) 2016/680) and states that any person may request information from the controller (data processor) as to whether personal data concerning them is being processed. Applied to the SIS, this means that any person in **Switzerland** can submit a request for access to data to fedpol (see Article 50 para. 1 N-SIS).

The data subject will be provided with the following **information** so that they can assert their rights:

- Identity and contact details of the controller
- Personal data processed, purpose of processing and legal basis
- Retention period / criteria for determining this period
- Origin of the personal data (if available)
- Information on the rights of data subjects, including contact details of the relevant supervisory authorities
- Information on any existing automated individual decision
- when disclosing personal data to third parties, the recipients



- in the case of disclosure of personal data abroad, the state / international body

Restriction, postponement, refusal of the right to information (Article 26 FADP and Article 15 LED):

a) **in general**, if

- a law provides for this (e.g. professional secrecy, ongoing criminal proceedings)
- overriding interests of third parties require this
- the request is manifestly unfounded or unlawful, or pursues a purpose contrary to data protection law

b) The person responsible is a **private individual**

- Overriding interests of the controller require it
- No disclosure to third parties

c) The person responsible is a **federal body**

- Overriding public interests (in particular the internal or external security of Switzerland) require it
- the information may jeopardise investigations / enquiries or official / judicial proceedings

Right to information in the **Schengen area**:

In principle, the same rights exist as listed above for Switzerland. In any country using the SIS, any data subject can apply to a court or competent authority for access, rectification or erasure of their data.

Modalities for requesting information (Article 50 N-SIS and Article 16 Data Protection Ordinance):

- Application in writing (electronically possible)
- Information is provided in writing (electronically possible) or in the form in which the data is available
- Possibly inspection on site
- Verbal disclosure of information only if the data subject agrees
- The controller must identify the data subject
- The person concerned is obliged to co-operate

Address:

Federal Office of Police fedpol
Crime prevention and law
Control and Planning Department
Coordination and Strategy Section



Guisanplatz 1A
CH - 3003 Bern

<https://www.fedpol.admin.ch> / [SIS information request \(admin.ch\)](#)

Notes:

The procedure for processing requests for information is governed by the national law of the Schengen state in which the request was submitted. In Switzerland, the answer must generally be given within 30 days, but at the latest within 60 days of the correct submission of the request.

The Federal Office of Police (fedpol) may, in accordance with Article 26 FADP (see also N (45) and (46) and Article 15 para. 1 and 3 LED) as mentioned above, refuse, restrict or postpone information. A request for information is potentially **abusive** if it pursues a purpose that is unrelated to data protection, e.g. avoiding the costs of obtaining evidence or information about a possible counterparty. A request for information is manifestly **abusive if** the right to information is repeatedly asserted without good reason or if the person addresses their request to a federal body which they know for a fact does not process any data about them.

A model letter for requesting access can be downloaded via the following link: [Request for access SIS](#).

➤ What are rights to rectification and erasure of data?

Both are regulated in Article 50 of the N-SIS Regulation. In principle, every person has the right to **have** incorrect personal data stored in the SIS **rectified or erased**.

Requests to rectify incorrect data stored in the SIS can be submitted to fedpol in Switzerland (see above) and to the competent national authority in the other Schengen states (see above).

The procedure for processing requests for rectification and erasure of data is governed by the national law of the Schengen state in which the request was submitted. In Switzerland, the person concerned must be informed of the measures taken no later than 3 months after the application has been correctly submitted.

Sample letters can be downloaded from the following link:

- [Request for rectification](#) SIS
- [Request for erasure of data](#) SIS

➤ Competent authority if an application was not / insufficiently complied with?

Each Schengen state has an authority that is responsible for handling **complaints** in connection with requests relating to data processing in the SIS. A distinction is made between the

- **Appeal** against an order (**legal remedy**) and the
- **Legal remedy** (the right to contact the FDPIC as supervisory authority in case of questions)



If your request is not honoured in Switzerland and there is no lawful reason for refusal, you have the **right to appeal**. The **decision in** which the requested authority informs you in writing that it will not comply with your application is a ruling. You can use this to lodge an **appeal with the Federal Administrative Court**.

If the competent authority in Switzerland does not grant a request for access, rectification or erasure within 60 days or three months of correct submission, you as the data subject may **appeal** in writing to the **Federal Data Protection and Information Commissioner (FDPIC)**.

Address:

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH - 3003 Bern
www.edoeb.admin.ch / [Contact form](#)

➤ Entitlement to compensation?

The person concerned may submit a **request for compensation** (Article 52 N-SIS) to the competent authority under national law in which they submit the request. The prerequisite is that an **alert** relating to the person concerned has been processed **unlawfully** in the SIS.

In Switzerland, this application must be submitted in writing to the **Federal Department of Finance**.

Address:

General Secretariat FDF
Federal Department of Finance
Bundesgasse 3
CH - 3003 Bern
www.efd.admin.ch / [Contact form](#)

➤ Who monitors data processing in the SIS?

In each Schengen state, a **national independent supervisory authority monitors** the lawfulness of the processing and transmission of personal data in the SIS for the national territory concerned.

In Switzerland, the **Federal Data Protection and Information Commissioner (FDPIC)** is responsible for this and monitors the federal bodies that use the SIS. Cantonal and communal users (e.g. the cantonal police) are monitored by the **cantonal data protection authorities**.

➤ Further questions about data protection claims?



In Switzerland, the FDPIC is the data protection supervisory authority for federal bodies (e.g. fed-pol).

- Federal Data Protection and Information Commissioner (FDPIC): www.edoeb.admin.ch

The following authorities are responsible for **Schengen**:

- European Data Protection Supervisor (responsible for data processing by EU authorities): [European Data Protection Supervisor \(europa.eu\)](http://europa.eu)
- Data protection authorities of the Schengen states (responsible for data processing by national authorities): [National Data Protection Authorities \(europa.eu\)](http://europa.eu)

Reference to the above statements concerning the Schengen area:

- [Alerts and data in the SIS - European Commission \(europa.eu\)](http://europa.eu)

Status: February 2024