Data protection notice for the Schengen Information System (SIS II)

Introduction

SIS II is a Europe-wide electronic system for searching for persons and objects, which is operated jointly by the Schengen states. It contains information on people wanted by the police and judicial authorities, people subject to an entry ban or missing people, as well as stolen objects (e.g. cars, weapons). SIS II is central to police and judicial cooperation.

Under the Schengen Agreement, systematic identity checks at the internal borders between Schengen countries have been abolished in order to facilitate travel. At the same time, cross-border police cooperation has been improved, thereby ensuring and strengthening security and order in the Schengen area.

Data protection notice

The **National Police** is responsible for the SIS II.

SIS II contains alerts on persons and objects. These alerts enable the competent authorities to identify a specific person or object and take the necessary measures. Since 2013, it has been possible to store biometric data such as fingerprints. Since the introduction of AFIS (Automated Fingerprint Identification System) in 2018, it has been possible to identify individuals solely on the basis of a comparison of their fingerprints.

The **National Police** is responsible for recording and transmitting the data within 72 hours outside the office hours of the Migration and Passport Office. In addition, the national police may request the comparison of fingerprints, facial images, or alphanumeric data in Eurodac for the purpose of preventing, detecting, or investigating terrorist or other serious crimes (in accordance with the annex to the Police Act). Only trained experts have access to the data and do the checks.

Alerts in SIS II concern:

- Third-country nationals (nationals of non-Schengen countries) who are refused entry to or stay in the Schengen area;
- People wanted for arrest for surrender or extradition purposes;
- Missing people (who may need to be taken into custody);
- people wanted for the purpose of participating in court proceedings;
- persons or objects for the purpose of discreet or specific checks;
- Items to be seized or preserved as evidence in criminal proceedings;
- Identity documents such as passports, identity cards, etc., which have been declared stolen, lost, or invalid;
- Vehicle documents, license plates, banknotes, securities and means of payment, weapons, caravans, trailers, industrial equipment, etc.

In Liechtenstein, the **National Police** force has access to SIS II data for the purpose of performing its duties in response to requests. It may provide the **Federal Customs Administration** with information on searches for persons or objects.

The **Migration and Passports Office** is also authorized to access the data for the purpose of performing its duties, but this is limited to querying data in connection with alerts issued by third countries for the refusal of entry and residence, and alerts for lost blank documents and identity documents.

Finally, the **Road Traffic Office** has the right to access the data. However, this is limited to searches for specific items such as motor vehicles, trailers, caravans, vehicle documents, and license plates.

The following **data** may be stored in SIS II:

- *Surname(s) and first name(s), maiden name(s) and previous name(s), as well as aliases;*
- *Distinctive physical characteristics;*
- *Date and place of birth;*
- *Sex;*
- *Photograph;*
- *fingerprints;*
- *nationality(ies);*
- *whether the person is armed or violent, or has escaped;*
- *reason for the alert;*
- *issuing authority;*
- *reference to the decision giving rise to the alert;*
- *action to be taken;*
- *Link(s) to other alerts in SIS II;*
- *The nature of the offense.*

Rights of a data subject in relation to data processed in SIS II

According to Chapter VI, B. of the N-SIS Regulation (LGBl. 2022 No. 306), the person has the following rights:

***Art. 30**: Exercising the right to information, correction, or deletion*

1) *If a person wishes to exercise their right to information, correction, or deletion, they must prove their identity and submit a written request to the state police. If the request is not submitted in person to the state police, persons residing abroad must enclose a certified copy of their passport with the request.*
    i. *The national police shall decide on the request after consulting the authority responsible for the alert. The national police shall decide on a request relating to incoming alerts after giving the Schengen State that issued the alert the opportunity to comment.*

2) *If the SIRENE bureau receives an opportunity from a Schengen state to comment on a request for information, correction, or deletion, it shall draft its comments in consultation with the authorities that requested or issued the alert.*
3) *If a person submits a request for **information**, they shall generally be informed within 30 days of receipt of their request. If the information cannot be provided within this period, the person shall be informed accordingly. However, the information must be provided no later than 60 days after the request for information was submitted.*
4) *If a person submits a request for **rectification** or **erasure**, they shall be informed of the decision taken no later than three months after submitting their request.*[1]

***Art. 31**: Right to information in the event of an alert for return or refusal of entry and stay*

1) *Third-country nationals who are the subject of an alert for return or refusal of entry and stay shall be provided with the **information** referred to in Articles 13 and 14 of Regulation (EU) 2016/679 ex officio.*
2) *The Migration and Passport Office shall transmit this information ex officio in text form together with its decision or order pursuant to Art. 13.*
3) *The information referred to in paragraph 1 may be omitted if:*
   a) *the personal data were not collected from the third-country national concerned and it is impossible or would involve a disproportionate effort to inform the person concerned;*
   b) *the third-country national concerned already has the information; or*
   c) *a restriction of the right to information is provided for in accordance with Art. 23 of Regulation (EU) 2016/679.*[2]

***Art. 29:** Principle*

1) *Subject to paragraph 2(b), data subjects may exercise their rights to access, rectification, and erasure by contacting the state police in accordance with Articles 57 and 58 of the Federal Act on Data Protection (FADP).*
2) *If the state police did not issue the alert themselves, the following applies:*
   a) *Information may only be disclosed if the Schengen state that issued the alert has been given the opportunity to comment beforehand.*
   b) *The data subject must be referred to the Schengen state that issued the alert in order to assert their right to rectification or erasure.*[3]

Further information can be found on the data protection office's website.

The Data Protection Authority is responsible for supervising the processing of EURODAC data in the Principality of Liechtenstein.

[1] Translated via DeepL; Please note that only the German version is legally binding.
[2] Translated via DeepL; Please note that only the German version is legally binding.
[3] Translated via DeepL; Please note that only the German version is legally binding.

Address of the competent authority:

Landespolizei des Fürstentums Liechtenstein
Postfach 684
Gewerbeweg 4
9490 Vaduz
tel: +423 236 71 11
email: https://www.landespolizei.li/kontaktformular