Media Scope Group

Overview of the Schengen Information System (SIS)

June 2024

Author: Dawid Wiktor

What is the Schengen Information System and how does it work?

The Schengen Information System (SIS) is a large-scale information system that supports security and border management in the European Union and the associated Schengen countries. It allows national authorities to share and access data on people and objects of interest, such as suspected criminals, missing persons, stolen vehicles, or firearms. It also facilitates the enforcement of return decisions and entry bans for third-country nationals who have no right to stay in the Schengen Area.

The Schengen Area is composed of 26 countries that have abolished internal border controls and allow free movement of people and goods across their territories. It includes 22 EU member states and four non-EU countries: Iceland, Liechtenstein, Norway, and Switzerland. The SIS is one of the main tools to compensate for the absence of internal border checks and to ensure a high level of security and cooperation within the Schengen Area.

The SIS was established in 1995 and has undergone several updates and enhancements since then. The current version, known as SIS II, was launched in 2013 and introduced new functionalities, such as the possibility to store biometric data (fingerprints and photographs) and to link different alerts. In March 2023, a new package of legal and technical changes entered into force, adding new alert categories, expanding the use of biometrics, and improving data quality and data protection.

The main features of the Schengen Information System

The SIS is a complex and versatile system that serves multiple purposes and offers various advantages for the countries that use it. Some of the main features of the Schengen Information System are:

- It is the largest and most widely used information system for security and border management in Europe, with over 90 million alerts stored and more than 6 billion queries made per year.
- It covers a vast geographical area, encompassing 29 countries and over 400 million people. It is also interoperable with other EU information systems and databases, such as the Visa Information System (VIS), the European Criminal Records Information System (ECRIS), and the Entry/Exit System (EES).
- It provides real-time and reliable information to national authorities, such as police, border guards, customs, and judicial officials. It enables them to identify and locate people and objects of interest during routine or random checks, as well as during investigations and operations.
- It supports the prevention and prosecution of serious crimes and terrorism, by allowing countries to share information on suspects, convicts, victims, witnesses, and potential threats. It also facilitates the execution of European Arrest Warrants (EAWs) and extradition requests among countries.
- It contributes to the protection of vulnerable persons, such as missing children or victims of trafficking, by allowing countries to issue alerts and request assistance from other

countries. It also allows countries to enter preventive alerts for persons who are at risk of abduction, violence, or harm.

- It enhances the management of external borders and migration, by allowing countries to issue alerts for third-country nationals who are subject to return decisions or entry bans, as well as for those who are refused entry or stay in the Schengen Area. It also helps countries to verify the validity and authenticity of travel documents and visas.
- It respects the fundamental rights and freedoms of individuals, by ensuring that the data stored and processed in the system are accurate, relevant, and lawfully entered. It also provides individuals with the right to access, correct, or delete their personal data, as well as to seek judicial redress and compensation in case of misuse or breach of data protection rules.

The components and actors involved in operation of the Schengen Information System

The SIS is composed of three main components: a central system, national systems, and a communication network. Each component has different roles and responsibilities, as well as different actors involved in its operation and supervision.

The central system

The central system, also known as CS-SIS, is the core of the SIS. It consists of a database that stores all the alerts and data entered by the countries that use the system, as well as a server that processes the queries and responses. The central system also contains a backup system, which ensures the continuity and security of the system in case of technical failures or emergencies.

The central system is managed by the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), which is responsible for ensuring its technical functioning, maintenance, and development. eu-LISA also monitors the performance and availability of the system, as well as the compliance of the countries with the technical and operational requirements.

The European Commission is responsible for the general oversight and evaluation of the SIS, as well as for adopting implementing and delegated acts on how the system works. The Commission also supports the cooperation and coordination among the countries and the EU agencies that use the system.

National systems

The national systems, also known as N-SIS, are the systems set up by each country that uses the SIS. They consist of a national copy of the central database, as well as the interfaces that allow the national authorities to enter, update, and consult the alerts and data in the system. The national systems also include the hardware, software, and procedures necessary to ensure the connection and communication with the central system.

The countries that use the SIS are responsible for setting up, operating, and maintaining their national systems and structures. They are also responsible for the content and quality of the alerts and data they enter and store in the system, as well as for the access rights and data protection rules they apply to their national authorities.

The national authorities that have access to the SIS vary depending on the country and the alert category. They typically include police, border guards, customs, immigration, judicial, and administrative authorities. They can enter and consult alerts and data in the system for the purposes of carrying out their tasks related to security, border management, migration, or judicial cooperation.

Communication network

The communication network, also known as s-TESTA, is the secure network that connects the central system with the national systems. It ensures the fast, reliable, and secure transmission of queries and responses between the countries and the central system, as well as among the countries themselves.

The communication network is also managed by eu-LISA, which is responsible for ensuring its technical functioning, maintenance, and development. eu-LISA also monitors the performance and availability of the network, as well as the compliance of the countries with the technical and operational requirements.

Functionalities and data types of the Schengen Information System

The SIS offers various functionalities and data types to support the different purposes and needs of the countries and the authorities that use it. The system allows the countries to share and access information on people and objects falling under one of the following alert categories:

- Return decisions: Alerts in respect of third-country nationals subject to return decisions issued by the countries.
- Refusal of entry or stay: Alerts covering third-country nationals who are not entitled to enter into or stay in the Schengen Area.
- Persons wanted for arrest: Alerts for people for whom a European Arrest Warrant or an extradition request has been issued.
- Missing persons: Alerts to find missing persons, including children, and to place them under protection if lawful and necessary.
- Children at risk of abduction: Alerts to prevent children at risk of being abducted by their own parents, relatives, or guardians from going missing.
- Vulnerable persons: Alerts to protect vulnerable people (adults or children) from being taken unlawfully abroad or to prevent them from travelling without the necessary authorizations.
- Persons sought to assist with a judicial procedure: Alerts to find out the place of residence or domicile of people sought to assist with criminal judicial procedures (for example, witnesses).
- Persons and objects for discreet, inquiry or specific checks: Alerts to obtain information on people or related objects for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security.

- Unknown wanted persons: Alerts containing only fingermarks and palmmarks belonging to a perpetrator of an offence discovered at the scenes of terrorist offences or other serious crimes under investigation.
- Objects for seizure or use as evidence in criminal procedures: Alerts on objects (for example, vehicles, travel documents, number plates, and industrial equipment) being sought for seizure or use as evidence in criminal proceedings.

Each alert contains a set of mandatory and optional data elements, depending on the alert category and the type of person or object concerned. The data elements may include identification data, alert reason, required action, criminal proceedings information, biometric data, and images. The data elements are structured and standardized to ensure consistency and interoperability among the countries and the authorities that use the system.

The Schengen Information System also allows the countries to link different alerts, for example, between a person and a vehicle, or between several persons related to the same case. This feature enables the authorities to obtain a more complete picture of the situation and to take coordinated actions.

The SIS uses biometric data, such as fingerprints, palm prints, fingermarks, palm marks, photographs, and DNA profiles, to confirm and verify the identity of people registered in the system. The system also allows the authorities to perform biometric searches, using the Automated Fingerprint Identification System (AFIS), to identify people based on their fingerprints or palm prints alone. This functionality increases the accuracy and reliability of the identification process and prevents the misuse or falsification of documents.

Safeguards and data rights

The SIS is subject to strict safeguards and rights to ensure the protection of the personal data stored and processed in the system, as well as the respect of the fundamental rights and freedoms of the individuals concerned. The system operates in compliance with the EU data protection rules and principles, as well as the international human rights standards and obligations.

The main safeguards and rights of the SIS are:

- Data quality: The countries that enter the alerts and data in the system are responsible for ensuring that they are accurate, updated, and lawfully entered and stored. They must also review and delete the alerts and data when they are no longer necessary or justified.
- Data security: The countries and the EU agencies that use the system are responsible for ensuring that the data is protected from unauthorized or unlawful access, modification, disclosure, or destruction. They must also report and investigate any data breaches or incidents that may affect the security or integrity of the system.
- Data supervision: The national data protection authorities supervise the application of the data protection rules in their respective countries, while the European Data Protection Supervisor monitors how the data protection rules are being applied in the

central system managed by eu-LISA. Both levels work together to ensure coordinated end-to-end supervision.

- Data access: The authorities that have access to the system must have a legitimate purpose and a legal basis to enter, update, and consult the alerts and data in the system. They must also respect the principle of proportionality and necessity and limit the access and use of the data to the minimum required for their tasks.
- Data rights: The individuals whose data are stored in the system have the right to request access to their data, as well as to correct or delete inaccurate or unlawfully stored data. They also have the right to seek judicial redress and compensation in case of misuse or breach of data protection rules.

These safeguards and rights can be exercised in any country that uses the SIS. The individuals can contact the national authority responsible for the SIS, the national data protection authority, or the court or competent authority of the country where they reside or where they are affected by the use of the system.

Frequently asked questions about the Schengen Information System

What is the Schengen Information System?

The Schengen Information System is a large-scale information system that supports border control and law enforcement cooperation in the Schengen States. The Schengen States are 26 European countries that have abolished internal border checks and allow free movement of people and goods within the area. The SIS enables competent authorities, such as police and border guards, to enter and consult alerts on persons or objects that are sought, missing or otherwise of interest. For example, the SIS can alert the authorities if a person is wanted for arrest, if a document is stolen or if a child is missing. The SIS also allows for the exchange of additional information and coordination through a network of national contact points called SIRENE Bureaux. The SIRENE Bureaux are responsible for providing supplementary information and facilitating the operational cooperation between the authorities in different countries.

Why is the SIS important for the EU and the Schengen Area?

The SIS is a key tool for ensuring security and freedom of movement within the EU and the Schengen Area. By providing timely and accurate information on people and objects of interest, the SIS helps the authorities to prevent, detect and investigate crimes and terrorism, to manage migration and asylum, and to protect vulnerable persons and victims. The SIS also contributes to the interoperability of EU information systems, which means that the systems can work together and share data in a secure and efficient manner. The interoperability of the SIS with other systems, such as the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), will enhance the security and management of the external borders of the EU and the Schengen Area.

Who is responsible for the SIS and how is it governed?

The SIS is a joint responsibility of the EU and the countries that use it. The European Commission ensures the overall functioning and development of the system, while eu-LISA, the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, operates and maintains the technical infrastructure. The EU Agency for Fundamental Rights (FRA) provides guidance and assistance on the respect of fundamental rights in the use of the system. The European Data Protection Supervisor (EDPS) supervises the processing of personal data by the EU institutions and bodies involved in the system. The national authorities of each country are responsible for entering, updating, deleting and consulting data in the system, as well as for ensuring data quality and data protection at national level. The national data protection authorities oversee the compliance with data protection rules by the national authorities. The Council of the EU and the European Parliament adopt the legal framework and the budget for the system, while the Court of Justice of the EU ensures the judicial review of the system.

How does the Schengen Information System protect personal data and fundamental rights?

The SIS is subject to strict data protection rules and safeguards that ensure the respect of the fundamental rights of the individuals whose data are stored in the system.

These include:

- Data quality: The data entered into the system must be accurate, up-to-date, relevant and not excessive for the purpose of the alert. The data must also be based on an existing decision or information from a reliable source. The authorities must regularly review and verify the data and delete it when they are no longer necessary or lawful.
- Data security: The data in the system is protected by appropriate technical and organizational measures against unauthorized access, alteration, disclosure, loss or destruction. Only authorized users can access the system and they must follow specific procedures and protocols. The system also records and monitors the activities of the users and generates logs and statistics that can be audited and controlled.
- Data protection: The data in the system is processed in accordance with the EU's General Data Protection Regulation (GDPR) and the specific data protection rules for the SIS. The EDPS and the national data protection authorities monitor the compliance with these rules and provide advice and guidance. The EU and the countries using the system must also appoint data protection officers who are responsible for ensuring the lawful processing of personal data in the system. The individuals whose data are stored in the system have the right to access, correct, delete, restrict or object to the processing of their data, as well as to lodge a complaint or seek a judicial remedy.

Summary

The Schengen Information System is a vital instrument for security and border management in the EU and the Schengen Area. It enables the countries and the authorities that use it to share and access information on people and objects of interest, as well as to cooperate and coordinate their actions. It also ensures the protection of personal data and the fundamental rights of the individuals concerned.

The SIS is constantly evolving and adapting to the changing needs and challenges of the EU and the Schengen Area. The latest update, which entered into force in March 2023, introduced new alert categories, expanded the use of biometrics, and improved data quality and data protection. The system will continue to develop and integrate with other EU information systems and databases to provide a more comprehensive and efficient service to the countries and the authorities that use it.

References

- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 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
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 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
- List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Article 41(8) of Regulation (EU) 2018/1861 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and Article 56(7) of Regulation (EU) 2018/1862 of the European Parliament and the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters
- List of N.SIS Offices and the national SIRENE Bureaux
- A Guide for Exercising Data Subjects' Rights: The Right of Access, Rectification and Erasure
- Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification)
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and repealing Council Framework Decision 2008/977/JHA
- Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast)
- Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network

- Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code)
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
- Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles
- Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226
- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data
- Council Framework Decision on the European arrest warrant and the surrender procedures between Member States
- What is the General Data Protection Regulation (GDPR)?

About Media Scope Group

Media Scope Group is an Estonian multinational integrated communications firm delivering services in the fields of public relations, public affairs, advocacy, marketing, data analytics, artificial intelligence and consulting.

www.mediascope.group | info@mediascope.group

Scan the QR code to visit our website.