European Commission

The Schengen Information System

June 2018

The Schengen Information System (SIS) is an EU information system to share information for law enforcement, border and migration management. It contains alerts on wanted or missing persons and objects such as vehicles, firearms, and identification documents that have been lost or stolen or may have been used to carry out a crime. Today, SIS is the most widely used security database in Europe, with over 5 billion consultations in 2017. It is an incredibly useful tool for police, border guards and customs officers. The system lies at the very heart of Schengen, and underpins the free movement of people within the area without internal border controls.

In December 2016, the Commission proposed to extend and improve the use of this database by enriching the data it contains with new alert categories. The proposal, on which co-legislators have now found an agreement, will ensure an even more efficient exchange of information between Member States, and with EU Agencies such as Europol, Eurojust and the European Border and Coast Guard Agency. At the same time, the security of personal data as it travels thought the SIS network, and as well as overall data protection safeguards, will be strengthened.

WHAT IS SIS USED FOR?

The main purpose of SIS is to help preserve internal security and improve border and migration management in the Schengen area by locating wanted persons and stolen objects and taking the necessary measures.

THREE AREAS OF COMPETENCE:

Border and migration management:

SIS enables border guards and migration authorities to enter and consult alerts on third-country nationals for the purpose of verifying their right to enter or stay in the Schengen Area.

NEW

Immigration authorities will now be required to enter return decisions and entry bans issued to irregular migrants into the database, increasing their EU- wide visibility.

Vehicle control:

Vehicle registration authorities have access to SIS. They can access alerts on stolen vehicles, number plates and vehicle registration documents, in order to check the legal status of vehicles presented to them for registration.

Security cooperation:

SIS supports police and judicial cooperation between Member States' authorities, by allowing them to create and consult alerts on missing persons, and on persons or objects related to criminal offences.

NEW

New alert categories such as those on unknown but wanted persons will enable the use of fingerprints found at a crime scene to identify and find people. Law enforcement officers will also for the first time be able to issue preventive alerts for children and vulnerable adults in need to protection.

Migration and Home Affairs

WHAT TYPE OF ALERTS CAN BE ISSUED?

EXISTING ALERTS

Refusal of entry or stay of third-country nationals

Persons wanted for arrest

Missing persons

Persons in order to assist with a judicial procedure

Persons and objects for discreet or specific checks

Falsified documents

Objects for seizure or use as evidence in criminal procedures

NEW ALERTS

Return decisions

Wanted Unknown Person alerts on the basis of fingerprints left at crime scenes

Persons and objects for inquiry checks

Preventive alerts to signal children at risk of parental abduction (under strict conditions)

WHAT KIND OF DATA IS ENTERED INTO SIS?

- **Data for identifying the person or object** that is the subject of the alert
- When available, **photographs and fingerprints**
- **Links between alerts** (e.g. between an alert on a person and a vehicle)

- **Use of facial images** for biometric identification
- **DNA profiles** for missing persons who need to be placed under protection, and especially for missing children

Information on why the person or object is sought

Instructions on the action to be taken when the person or object has been found

WHICH AUTHORITIES CAN ENTER AND SEARCH ALERTS IN SIS?

- National border control authorities,
- Police authorities,
- Customs authorities,
- Judicial authorities,
- Visa and immigration authorities
- Vehicle, (NEW) **boat and aircraft** registration authorities

Exclusively accessible to the authorised users within competent national authorities.

NEW Europol

will receive access to all alert categories in SIS, including on data on missing persons, return alerts, and third-country nationals whose entry or stay is refused in the Schengen area and will be included in the exchange of supplementary information in relation to SIS alerts that have been issued within the context of serious organised crime and terrorism.

Eurojust

can continue to access the system to carry out queries on the alert categories it needs to access for its work.

NEW European Border and Coast Guard Agency

The new Agency and its teams will have access to all alert categories in SIS, which will allow them to do their jobs more effectively, when carrying out returns of irregular migrants and managing the future European Travel Information and Authorisation System.

IN WHICH COUNTRIES IS SIS IN OPERATION?

EU Member States that are part of the Schengen Area

Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland)

Special conditions exist for EU Member States that are not part of the Schengen Area (Bulgaria, Romania, and the United Kingdom). SIS is not yet operational in Cyprus and Ireland, but work is underway to fulfil the technical and legal conditions for them to receive partial access to SIS.

HOW IS DATA PROTECTION ENSURED?

SIS has **strict requirements on data quality and data protection**. The basic principle is that the country entering an alert is responsible for its content, and that alerts are only kept for the time required to fulfil the purpose for which they were issued (e.g. an arrest).

National Data Protection Authorities

supervise the application of the data protection rules

European Data Protection Supervisor

monitors the application of the data protection rules for the central system

Both levels cooperate to ensure coordinated end-to-end supervision.

If data about a person are stored, that person has the **right to request access to this data and make sure that it is accurate and lawfully entered. If this is not the case, the person has the right to request correction or deletion.**

NEW **Additional safeguards** are introduced to ensure that the collection, processing and access to data is limited to what is strictly necessary and operationally required; and in full respect of EU data protection legislation and fundamental rights. **Access is restricted to those officials who have an operational need to process it**.