

The Schengen Information System

21 December 2016

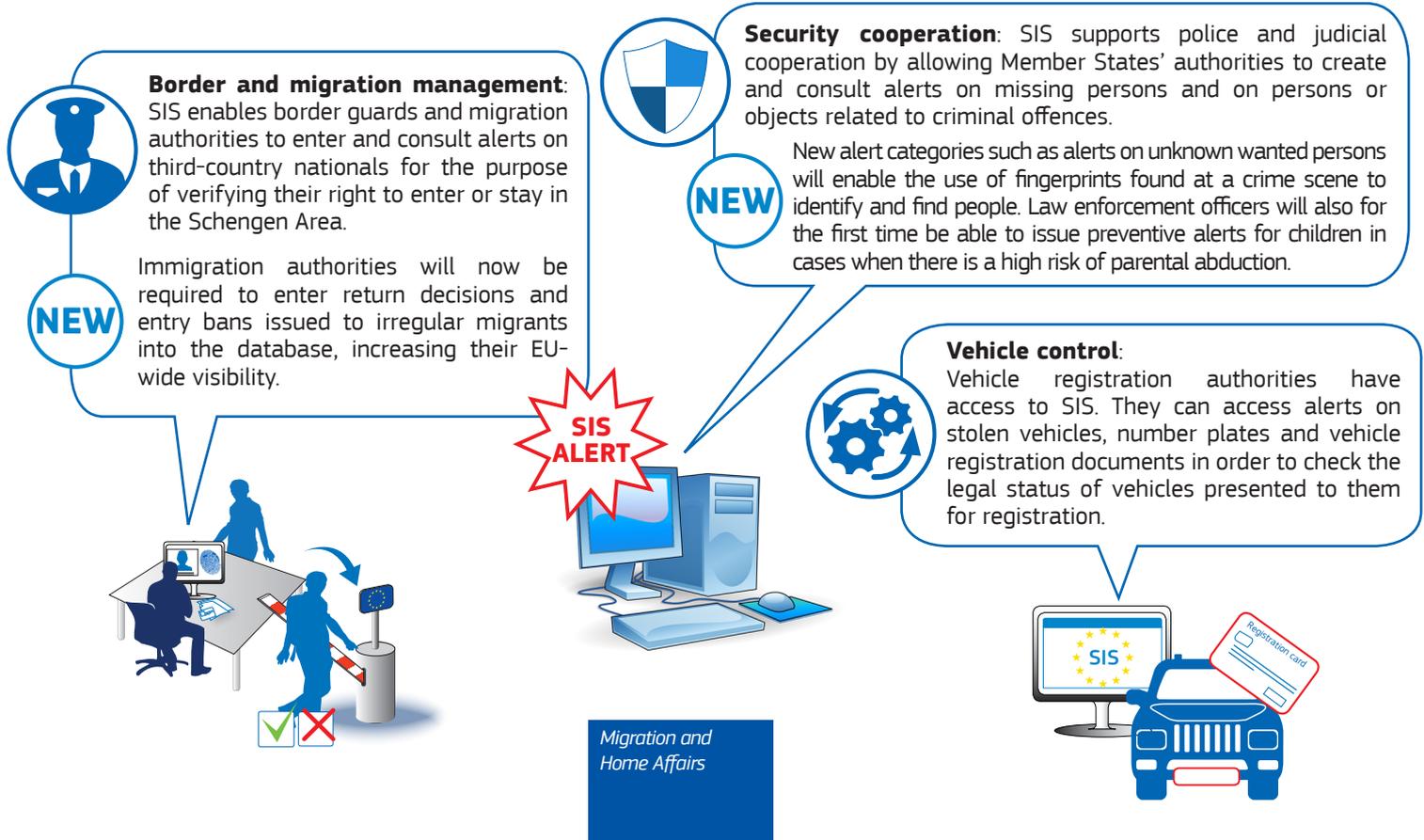
The Schengen Information System (SIS) is an EU information system to share information for law enforcement, border and migration management. It contains alerts on wanted or missing persons and objects such as vehicles, firearms, and identification documents that have been lost or stolen or may have been used to carry out a crime. Since its creation over 15 years ago the SIS database has proven to be an incredibly useful tool for police, border guards and customs officers - who all need to have access to high quality information about the persons or objects they are checking, with clear instructions about what needs to be done in case of a hit with SIS. The system is at the very heart of Schengen cooperation and plays a crucial role in facilitating the free movement of people within the Schengen area.

The Commission is now proposing to extend and improve the use of this database by enriching the data it contains with new alert categories, ensuring an even more efficient information exchange between Member States and with EU Agencies such as Europol, Eurojust and the European Border and Coast Guard, improving the end-to-end security of the system and strengthening data protection safeguards.

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:



WHAT TYPE OF ALERTS CAN BE ISSUED?

EXISTING ALERTS



NEW ALERTS



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 (Note: only possible in the absence of photographs or fingerprints suitable for identification)

NEW

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 job more effectively in carrying out returns of irregular migrants and managing the future European Travel Information and Authorisation System.

IN WHICH COUNTRIES IS SIS IN OPERATION?

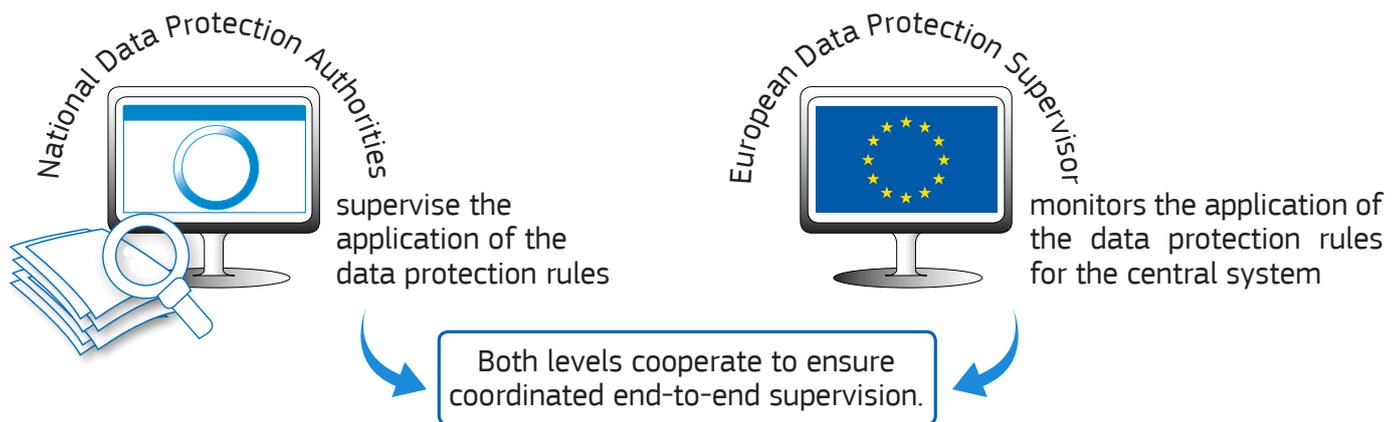
EU Member States that are part of the Schengen Area

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 Croatia, Cyprus and Ireland, but work is underway to fulfil the technical and legal conditions for them to connect 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).



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, in full respect of EU legislation and fundamental rights, including the right to effective remedies. **Access is restricted only to those who have an operational need to process it.**