Council of the European Union

Brussels, 24 February 2023
(OR. en)

6660/23

JAI 188
IXIM 31
SIRIS 21
COMIX 92

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Entry into operation of the enhanced SIS

A new SIS for a new era

On 7 March 2023, the Schengen Information System (SIS) is enhanced with new functionalities. Building on the experience gained over years of operation, a new legal framework[1] will ensure that the SIS continues to effectively tackle changing, diverse forms of serious crime, terrorism and migration challenges in the years to come.

The SIS is the most important information exchange system for security and border management in the Union, used by millions of users in their daily work[2]. It allows law enforcement authorities, border authorities and EU agencies to share information in a timely manner and to support operational cooperation, ensuring a high level of security in the Union, as well as contributing to migration management.

1 Regulations (EU) 2018/1860, 2018/1861 and 2018/1862 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; on the establishment, operation and use of the Schengen Information System in the field of border checks; and on the establishment, operation and use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters (OJ L 312, 7.12.2018, p. 1, p. 14, p. 56).

2 The SIS contains alerts on more than one million persons who are either wanted for different reasons or are subject to a refusal of entry and stay in the Schengen area. Furthermore, the system contains alerts on over 86 million lost or stolen objects. In 2022 alone, competent authorities consulted the SIS almost 35 million times a day. There were 263 452 hits on foreign alerts, the majority of which were on persons detected.

The new SIS maximises its effectiveness with more categories of data, including biometrics, and new types of alerts. It addresses potential gaps and provides access to a greater number of national authorities and EU agencies.

Enhancements by policy area

In the area of **police cooperation** for the prevention, detection, investigation and prosecution of criminal offences (and the execution of criminal penalties), the new SIS provides a strengthened toolbox to counter cross-border crime.

For example, for the first time, the SIS contains biometric information not linked to known individuals that will help to identify perpetrators. Fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences will be entered into the SIS in the form of new alerts on unknown suspects or wanted persons.

Also for the first time, DNA profiles are included to facilitate the identification of missing persons in cases where fingerprint data, photographs or facial images are not available or not suitable for identification.

New alerts issued for the purpose of inquiry checks allow national authorities to collect relevant information, in order to help them with their ongoing investigations.

The possibilities to insert new types of objects and more identifiable numbers on stolen objects improve the chances of identification and repatriation to the legal owners.

Another important development is that **national migration authorities** get full access to the SIS, contributing to an effective border control, the facilitation of legitimate border crossings and, where appropriate, measures to efficiently fight cross-border crime at the external borders, in particular migrant smuggling, trafficking in human beings, and terrorism.

The introduction of a new type of alert on return decisions issued to illegally staying third-country nationals is expected to provide a comprehensive overview of all return decisions issued in the Schengen area.

The new SIS also aims to **protect vulnerable persons** who need to be prevented from travelling. New preventive alerts help to identify children at risk of parental abduction, persons at risk of different forms of gender-based violence, or of being involved in terrorist offences or enlisted into armed groups.

Wider access rights are also granted **to other national authorities** (e.g. competent national authorities responsible for the issuance of work permits, long-term visas, naturalisation, registration services for boats, aircrafts or firearms).

Additionally, several EU agencies will have wider access to the SIS to allow them to deliver on their extended mandates.

Europol has full access to all categories of data in the SIS, enabling the agency to further support Member States. When a person is sought in relation to a terrorist offence, national authorities inform Europol of any hits, allowing Europol's Operational Centre to check if there is any additional contextual information available in Europol's databases. In addition, Europol continues to exchange supplementary information with Member States via the SIRENE Bureaux.

Likewise, **Frontex**'s teams will have full access to all categories of data in the SIS and **Eurojust** will have an extended access to new alerts on unknown wanted persons.

Challenges and opportunities

A new phase for the SIS starts and further developments and improvements are in the pipeline. In a few years, the SIS will incorporate a new type of information alert to record information on third-country nationals provided by third parties.

The SIS is the first building block of the project for the Interoperability of large-scale IT systems in the area of freedom, security and justice. In this respect, it is of vital importance that the insertion of biometrics (dactyloscopic data, DNA, facial images) in the SIS is continued and increased to maximise the benefits of its integration with the Interoperability components.

Given the wider scope of the enhanced SIS, a number of challenges need to be considered in view of its smooth implementation.

Firstly, work needs to continue after 7 March 2023 to exploit in full the new possibilities brought by the SIS. The beginning of operations is not exempt from technical issues regardless of the extensive testing carried out at central and national levels. Therefore, Member States' authorities and eu-LISA are reminded to remain vigilant during the first phase of the rollout. This will be followed by a gradual fine-tuning of business processes in the context of the continuous improvement of the tool.

Secondly, the implementation of some of the new types of alert (inquiry checks, preventive alerts) has proven to be challenging as considerable differences have been observed at national level. Member States need to continue to explore ways to further develop a harmonised approach to implement the new legal framework while complying with their national laws. In this respect, close coordination among Member States and the eventual adaptation of secondary legislation and of key deliverables (SIS handbook, SIRENE manual) needs to continue.

Thirdly, the deployment of the enhanced SIS translates into an increased workload in all SIRENE Bureaux, which will likely be intensified with the deployment of the EES, ETIAS and Interoperability. The increased workload has to match adequate financial and human resources. The new SIS being a genuine asset, investments in the SIRENE Bureaux bring tangible benefits.

Taking into account the expected gains resulting from the enhanced SIS, the Presidency supports eu-LISA, the Commission and Member States' authorities to ensure a smooth implementation and a progressive use of all new features. The Presidency underlines the importance of maintaining an ambitious approach in order to strengthen the operational cooperation between Member States' authorities and with EU agencies to ultimately preserve the area of freedom, security and justice.