Security Union: Technical and operational updates of the Schengen Information System – Questions & Answers

Brussels, 21 December 2016

.

What is the Schengen Information System?

The Schengen Information System (SIS) is a centralised, large-scale information system that supports border controls at the external Schengen borders and law enforcement and judicial cooperation in 29 countries throughout Europe. The Schengen Information System was set up in 1995 to contribute to maintaining internal security and fighting cross border crime and irregular migration following the abolition of internal border controls.

SIS stores alerts and provides information on wanted persons or objects. The system contains information on individuals who do not have the right to enter or stay in the Schengen area, or those who are sought in relation to criminal activities. It also contains information on missing persons, in particular children and other vulnerable individuals who are in need of protection. Details of certain objects are also recorded in SIS; for example, vehicles, firearms, boats and identification documents that have been lost or stolen or may have been used to carry out a crime.

SIS contains data that is needed to locate a person and confirm his/her identity, including photographs, fingerprints and, as part of today's proposed changes, palm prints and DNA profiles (under particular and limited circumstances related to missing persons). The system also includes instructions to the police officer or border guard on the specific action to be taken when the person or object is located, for example to arrest a person, protect a vulnerable missing person or to seize an object, such as an invalid passport or stolen car.

According to the evaluation of SIS carried out by the Commission in 2016 and presented today, the system is operating effectively and has been an outstanding operational and technical success. No other law enforcement cooperation system generates as many positive outcomes or can handle as much information flow in real time with the result that, year on year and in all alert categories, hits have increased substantially. Building on this success, the evaluation report also set out some areas where operational and technical improvements could be made. The proposals presented today are following up on the recommendations of the evaluation report.

What are the main improvements proposed by the Commission today?

The proposals presented today will strengthen the protection of personal data, bringing it into line with the new Data Protection Regulation. The security of the system is improved, with strict legal requirements for uninterrupted operations, incident management processes and better training for end-users. National supervisory authorities and the European Data Protection Supervisor are given an explicit role in ensuring that data is protected properly and Member States are liable for penalties if breaches cause damage to a person (for example if factually inaccurate data is entered or if data is stored unlawfully).

In particular, the changes proposed by the Commission today will:

- improve the security and accessibility of the system by providing for uniform requirements for officers on the ground on how to process SIS data in a secure way and ensure business-continuity for end-users;
- strengthen data protection by introducing additional safeguards to ensure that the collection and processing of and access to data is limited to what is strictly necessary, in full respect of EU legislation and fundamental rights, including the right to effective remedies;
- improve information sharing and cooperation between Member States, notably through the introduction of a new alert category on "unknown wanted persons" and full access rights for Europol ;
- help combat terrorism by introducing the obligation to create a SIS alert in cases related to terrorist offences and a new 'inquiry check' to help authorities gather essential information;

- better protect children by allowing authorities to issue, in addition to alerts for missing children, preventive alerts for children who are at high risk of abduction;
- contribute to the effective enforcement of entry bans for third-country nationals at the external border by making their introduction in the SIS compulsory;
- improve the enforcement of return decisions issued to irregularly staying third-country nationals by introducing a new alert category for return decisions;
- make more effective use of data such as facial imaging and palm prints to identify persons entering the Schengen area;
- strengthen the support for prevention and investigation of theft and counterfeiting by providing for alerts to be issued on a wider range of stolen and falsified goods and documents.

Which alert categories are the Commission proposing to add? What is their added value?

The Commission is proposing to add the following categories to the system:

- **Preventive alerts on children at risk of parental abduction:** Changes to the alerts on missing persons will allow for preventive alerts to be issued in cases where **parental abduction** is deemed a high risk and upon request by a judicial authority, and provide for more **finely tuned categorisation** of alerts for missing persons. These changes address a potential gap in the current legislation whereby alerts for children can only be issued once they are already missing. It will allow authorities in Member States to indicate children at particular risk and inform border guards and law enforcement of the existence of such a risk – allowing them to take a traveling at-risk child into protective custody if required. This alert will require a decision, in respect of the best interests of the child, by the relevant judicial authorities granting custody only to one of the parents and where there is an imminent risk of abduction.
- **Alerts for unknown persons wanted in connection with a crime:** The proposed changes will allow SIS alerts to be issued for **unknown persons wanted in connection with a crime**, based on fingerprints or palm prints. These alerts may be created in cases where, for example, latent fingerprints or palm prints are discovered at the scene of a serious crime and where there are strong reasons to suspect that the fingerprints belong to the perpetrator of that crime. These alerts can only be issued if the identity of the person cannot be established by using any other national or European/international databases which store fingerprints.
- **Expansion of the alerts on objects:** The **list of objects for which alerts can be issued** is expanded, adding falsified documents, vehicles regardless of propulsion system (i.e. electric as well as petrol/diesel), counterfeit banknotes, IT equipment and identifiable component parts of vehicles and industrial equipment.
- **Alerts on refusal of entry and stay:** The conditions for issuing alerts on refusal of entry and stay are amended to ensure consistency with the provisions of the Return Directive (Directive 2008/115/EC). With the proposed changes, it will become mandatory to enter alerts in SIS in cases where an entry ban has been issued to an irregularly staying third-country national in accordance with the Return Directive in order to deny entry to the Schengen area during a defined period of time starting from the moment of departure of third-country national concerned.
- **Alerts for the return of irregularly staying third-country nationals:** The proposed changes require the creation of a SIS **alert for persons for whom a return decision has been issued** by the competent national authorities in accordance with provisions respecting the Return Directive. Making use of SIS for returns will:
- support immigration authorities in following up on and enforcing return decisions issued to third-country nationals who have no right to stay in the Member States;
- help to prevent and deter irregular migration; and
- improve information sharing and cooperation between immigration authorities.

Are Member States increasingly making more use of the system?

At the end of 2013, there were just over 50 million alerts in the system. By November 2016, that number had grown to nearly 70 million. SIS was accessed by the competent authorities 2.9 billion times in 2015, one billion times more than in 2014. This trend can be expected to continue, as the proposed changes expand the categories of alerts that can be issued, making the system even more useful for Member States.

A 'hit' in SIS II means that the person or object has been found in another Member State and further

action, specified in the alert, is provided by the system. Between the entry into operation of SIS II on 9 April 2013 and the end of 2015 over 371,000 hits were achieved (an average of over 370 hits per day).

This equates to:

- Over 25,000 people arrested to face justice in another Member State.
- Over 79,000 people refused entry or stay in the Schengen area (having already been subject of a decision on refusal of entry or stay).
- Over 12,000 missing persons found having crossed a border into another Member State.
- Over 83,000 people traced to assist with a criminal judicial procedure.
- Over 72,000 travelling serious criminals and other people posing threats to security located.
- Over 97,000 cases solved concerning stolen motor vehicles, misuse of identity or travel documents, stolen firearms, stolen number plates and other lost or stolen property.

How does the proposal strengthen personal data protection?

The proposals presented today will strengthen the protection of personal data, bringing it into line with the new data protection regulation. The security of the system is improved, with strict requirements in the legislation for business continuity arrangements and incident management processes and better training for end-users. This will ensure greater protection for the data stored within the system.

Additional safeguards are introduced to ensure that the collection and processing of 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 to those who have an operational need to process it. The proposals set out clear data retention timeframes and provision for individuals' rights to access and rectify data relating to them and to request erasure in line with their fundamental rights.

National supervisory authorities and the European Data Protection Supervisor are given an explicit role in ensuring data is protected properly and Member States are liable for penalties if breaches cause damage to a person (for example if factually inaccurate data is entered or if data is stored unlawfully).

Who is authorised to enter and search alerts in SIS?

The SIS is a highly secure and protected database that is accessible exclusively to authorised users within relevant competent authorities, such as national border control, police, customs, judicial, visa and vehicle registration authorities to carry out checks and create alerts. These authorities may only access the SIS data which is relevant for the performance of their tasks. The proposal allows access to authorities responsible for the registration of aircraft and boats to carry out their tasks related to the registration.

The European agencies Europol and Eurojust have access rights to carry out certain types of queries on specified alert categories. The proposals expand Europol's access rights, allowing it to additionally access missing persons alerts and alerts issued for a criminal judicial procedure, in order to allow Europol officials to better carry out their duties. The proposals also give the new European Border and Coast Guard Agency access to SIS and SIS data to the extent necessary to carry out its mandate and for its staff to perform their verification duties in the context of the Commission's proposal establishing a European Travel Information Authorisation System (ETIAS).

How does the proposal strengthen the rights to access personal data in SIS?

The proposals explicitly recognise the rights to access personal data that is stored in SIS, to correct the data if it is inaccurate and to have it deleted if it should not be stored. Persons also have the explicit right to bring proceedings before the courts or competent authorities to correct or delete data and/or obtain compensation.

These rights can be exercised in any Member State, regardless of which authority entered the data into SIS, and the competent authorities must respond to an access request within 60 days. Details of national procedures and contact points for access requests can be found in a comprehensive guide that is available on the EDPS website.

How is an alert issued?

The system has three major components:

- a central system;
- national systems; and

- a communication infrastructure (network) between the central system and the national systems.

These work together, so that an alert which is entered in SIS in one country is transferred in real time to the central system. The new alert will then appear when a relevant search is made, no matter which country the search is being carried out in.

How is SIS managed?

Each country using SIS is responsible for setting up, operating and maintaining its national system and its national SIRENE Bureau.

The EU Agency for large-scale IT systems, eu-LISA, is responsible for the operational management of the central system and the communication infrastructure.

The European Commission is responsible for the general oversight and evaluation of the system, including the correct application and implementation of its legal framework, and for the adoption of implementing measures such as the rules for entering and searching data.

Additionally, the SISVIS Committee, comprised of technical and operational experts from the Members States and chaired by the Commission, harmonises operational procedures in order to optimise the use of SIS and enables the exchange of best practice between Member States.

How much will these changes cost?

The overall additional cost for implementing these changes between 2018 and 2020 is expected to be **€67.9 million**. This consists of €64.3m for technical upgrades, increasing the capacity of the TESTA-NG network and upgrades to national systems to implement the provisions relating to law enforcement and border issues, while €3.6m will be needed for technical upgrades relating to returns issues.

To which Member States do the SIS provisions apply and in which ways?

Police and judicial cooperation: The SIS provisions related to police and judicial cooperation (for example alerts on missing persons) apply in all EU Member States that are connected to SIS, including the UK, Romania and Bulgaria and the Associated Countries who are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland).

These provisions are **not yet operational** in Ireland, Cyprus and Croatia.

Border checks (Schengen area): The provisions related to border checks (for example alerts on refusal of entry and stay) apply in all EU Member States and Associated Countries (Switzerland, Norway, Liechtenstein and Iceland) that are part of the Schengen area.

They **do not apply** to theUK and Ireland, who do not have the right to opt in either. In addition, the provisions do not apply to Romania, Bulgaria, Croatia and Cyprus as they are not yet part of the Schengen area.

Return: The provisions on return (alerts on return decisions) apply inall EU Member States (including Bulgaria and Romania) and the Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland).

They **do not apply** to the UK and Ireland, which have the right to opt in under certain conditions.

What are the next steps?

The three proposed Regulations will be sent to the European Parliament and the Council for discussion and adoption, in line with the normal legislative process.

Once adopted, the new Regulations will come into effect once all the necessary technical and legal arrangements have been made to implement the changes in the proposals – expected for 2021.

For more information

Press release

Factsheet: Schengen Information System (SIS)

Proposals to improve the operational effectiveness and efficiency of the Schengen Information System (SIS):

- in the field of police cooperation and judicial cooperation in criminal matters
- in the field of border checks
- for the return of illegally staying third country nationals

Evaluation report of the second generation Schengen Information System (SIS II)

Commission Staff Working Document accompanying the evaluation Report

Communication on Stronger and Smarter Information Systems for Borders and Security

Communication delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union

Press release: State of the Union 2016: Commission Targets Stronger External Borders

Frequently asked questions: State of the Union 2016: Paving the way towards a genuine and effective Security Union – Questions & Answers

Press release: Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System

Frequently asked questions: Smart Borders package

Factsheet: Stronger and Smarter borders for the European Union. The Entry-Exit System

Press release: Commission launches discussion on future framework for stronger and smarter inform

MEMO/16/4427

Press contacts:

Natasha BERTAUD (+32 2 296 74 56)
Tove ERNST (+32 2 298 67 64)
Kasia KOLANKO (+ 32 2 296 34 44)
Markus LAMMERT (+ 32 2 298 04 23)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email