Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters

2016/0409(COD) - 24/10/2018 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 555 votes to 67, with 20 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of 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, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amended the Commission proposal as follows:

Purpose: the proposed Regulation seeks to introduce a **series of improvements to SIS** which shall increase its effectiveness, strengthen data protection and extend access rights. It establishes the conditions and procedures for the entry and processing of alerts in SIS on **persons and objects** and for the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.

Technical architecture: SIS includes a central system (Central SIS) and national systems. The national systems may contain a complete or partial copy of the SIS database, which may be **shared by two or more Member States**. The availability of SIS shall be subject to close monitoring at central and Member State level and any incident of unavailability for end-users shall be registered and reported to stakeholders at national and Union level. Each Member State shall set up a **backup** for its national system.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (**eu-LISA**) shall implement technical solutions to reinforce the uninterrupted availability of SIS.

Member States' responsibilities: each Member State shall designate a national authority which is **operational 24 hours a day, 7 days a week** and shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau). The SIRENE Bureau shall serve as **single contact point** for Member States to exchange supplementary information regarding alerts.

Each SIRENE Bureau shall, in accordance with national law, have easy **direct or indirect access** to all relevant national information, including national databases and all information on its Member States' alerts, and to expert advice, in order to be able to react to requests for supplementary information swiftly and within the deadlines. Member States shall ensure that end-users and the staff of the SIRENE Bureaux regularly receive **training**, including on data security, data protection and data quality.

Data security: Parliament specified that **national plans for security**, business continuity and disaster recovery shall ensure that: (i) **unauthorised processing** of data in the SIS and any unauthorised modification or erasure of data processed in the SIS is prevented; (ii) systems installed in the event of an interruption are **restored**; (iii) the SIS correctly performs its functions, that faults are reported and **personal data** stored in SIS cannot be corrupted by means of the system malfunctioning.

Where a Member State cooperates with **external contractors** in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular on security, confidentiality and data protection.

Categories of data: the amended text provides for the introduction of new categories of data in the SIS to enable end-users to make informed decisions based on an alert without losing time.

In order to facilitate identification and detect multiple identities, the alert shall, where such information is available, include a reference to the **personal identification document** of the individual concerned or its number and a copy, if possible in colour, of the document. Where available, all the relevant data, in particular the **forename of the individual concerned**, shall be inserted when creating an alert.

Alerts: alerts on the following categories of persons shall be entered in SIS at the request of the competent authority of the issuing Member State:

- missing persons who need to be placed under protection for their own protection and in order to prevent a threat to public order or public security;
- children at risk of abduction by a parent, a family member or a guardian, who need to be prevented from travelling;
- children who need to be prevented from travelling owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and (i) becoming victims of trafficking in human beings, or of forced marriage, female genital mutilation or other forms of gender-based violence; (ii) becoming victims of or involved in terrorist offences; or (iii) becoming conscripted or enlisted into armed groups;
- vulnerable persons who are of age and who need to be prevented from travelling for their own protection owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings or gender-based violence.

Actions and decisions by the competent authorities, including judicial authorities, following an alert on a child should be taken in cooperation with child protection authorities. The national **hotline** for missing children should be informed, where appropriate.

Within **three years** of entering an alert in the SIS, the issuing Member State shall review the need to keep it.

Biometric data: under the proposed Regulation, SIS shall permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned.

Parliament has specified that any entry of photographs, facial images or dactyloscopic data into SIS and any use of such data shall: (i) be **limited to what is necessary** for the objectives pursued; (ii) be authorised by Union law; (iii) respect **fundamental rights**, including the best interests of the child; (iv) be in accordance with Union law on **data protection**.

It would also be possible to add a **DNA profile** to an alert in clearly defined cases where fingerprint data are not available. This DNA profile shall only be accessible to authorised users.

Access to the system: the proposed Regulation provides for enhanced access possibilities for a range of European agencies such as Europol, Eurojust, and the European Border and Coast Guard Agency.

The amendments adopted aim to clarify, with regard to the existing mandates of the different agencies, the circumstances under which access to SIS data is possible.