Schengen Information System (SIS) in the field of border checks

2016/0408(COD) - 24/10/2018 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 530 votes to 50, with 66 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 border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006.

The European Parliaments 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 third-country nationals and for the exchange of supplementary information and additional data for the purpose of refusing entry into and stay on the territory of the Member States.

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.

Costs: the amended text provides that funding shall be allocated from the envelope of EUR 791 million foreseen under Regulation (EU) No 515/2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa, to cover the costs of implementation of this Regulation. From this envelope, an amount of EUR 31 098 000 is allocated to eu-LISA. Member States shall receive an additional global allocation of EUR 36 810 000 to be distributed in equal shares through a lump sum to their basic allocation.

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 on refusal of entry and stay: an alert may only be entered if the Member State has taken an administrative or judicial decision and has concluded, after an individual assessment, that the third-country national constitutes a threat to public policy or public security or national security, namely where:

- a third-country national has been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year;
- there are serious grounds for believing that a third-country national has committed a serious criminal offence, including a terrorist offence, or there are clear indications of his or her intention to commit such an offence in the territory of a Member State;
- a third-country national has circumvented or attempted to circumvent Union or national law on entry into and stay on the territory of the Member States.

Retention period: within three years of entry of an alert into SIS, the issuing Member State shall review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five years.

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.

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.

In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters, where monitoring of their movement is crucial, Member States are encouraged to share information on terrorism-related activity with Europol. This information sharing should be carried out through the exchange of supplementary information with Europol on the alerts concerned.