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

2016/0408(COD) - 28/11/2018 - Final act

PURPOSE: to improve the Schengen Information System (SIS) in the field of border checks with a view to making it more efficient, strengthening data protection and extending rights of access.

LEGISLATIVE ACT: Regulation (EU) 2018/1861 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, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

CONTENT: the Schengen Information System (SIS) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union. This Regulation:

- 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;

- lays down provisions on the technical architecture of SIS, on the responsibilities of the Member States and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), on data processing, on the rights of the persons concerned and on liability.

The Regulation is accompanied by two other Regulations on the use of the SIS: (i) in the field of police and judicial cooperation in criminal matters; (ii) for the purpose of returning illegally staying third-country nationals.

Architecture

SIS comprises a central system (Central SIS) and national systems. National systems may contain a full or partial copy of the SIS database, which may be shared by two or more Member States. The Central SIS and the communication infrastructure will have to be managed so as to ensure their functioning 24 hours a day, 7 days a week. For this reason, the Agency "eu-LISA" will implement technical solutions to reinforce the continuous availability of SIS.

New categories of data

New data categories are introduced in SIS to allow end-users to take informed decisions based upon an alert without losing time. Alerts for refusal of entry and stay should contain information concerning the decision on which the alert is based. Furthermore, in order to facilitate identification and detect multiple identities, the alert should, 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.

Alerts for refusal of entry and stay

An alert may be entered only if the Member State has taken an administrative or judicial decision and has concluded, after an individual assessment, that the third-country national poses a threat to public policy or public security or to national security, namely when:

- a third-country national has been convicted in a Member State of an offence punishable by deprivation of liberty for at least one year;

- there are serious reasons to believe that a third-country national has committed a serious criminal offence, including a terrorist offence or if it appears that he intends to commit such an offence in the territory of a Member State;

- a third-country national has circumvented or attempted to circumvent national or Union law on entry and residence in the territory of the Member States.

The issuing Member State shall ensure that the alert takes effect in SIS as soon as the third-country national concerned has left the territory of the Member States.

Biometric data

SIS will permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. Any entry of photographs, facial images or dactyloscopic data into SIS and any use of such data should: (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, and (iv) be in accordance with Union law on data protection.

In order to avoid inconveniences caused by misidentification, SIS should also allow for the processing of data concerning individuals whose identity has been misused, subject to suitable safeguards, to obtaining the consent of the individual concerned for each data category, in particular palm prints, and to a strict limitation of the purposes for which such personal data can be lawfully processed.

Period for keeping alerts

An issuing Member State shall, within three years of the entry of an alert into SIS, 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.

Access to data

Europol will have access to all categories of data contained in the SIS and may exchange additional information with the SIRENE Bureaux of the Member States. In addition, Member States must inform Europol of any positive response when a person is wanted in connection with a terrorist offense. The European Border and Coast Guard Agency will also have access to the different categories of alerts in the SIS. This will allow Europol's European Counter Terrorism Centre to check if there is any additional relevant information available in Europol's databases.

For the purposes set out in its mandate, the European Border and Coast Guard Agency will also have access to the alert categories in SIS.

ENTRY INTO FORCE : 27.12.2018.

By 28.12.2021, the Commission shall adopt a decision setting the date on which the SIS is put into service under the Regulation after verifying that the relevant conditions are fulfilled.