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

2016/0409(COD) - 28/11/2018 - Final act

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

LEGISLATIVE ACT: Regulation (EU) 2018/1862 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 and repealing Council Decision 2007 /533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

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 persons and objects and for the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters;

- 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 SIS: (i) in the field of border checks ; (ii) for the return of 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 category of alerts

The following are introduced into the system:

- alerts issued for the purpose of inquiry checks, an intermediary step between discreet checks and specific checks, which allow for individuals to be interviewed.

- alerts on unknown suspects or wanted persons, which provide for the introduction into the SIS of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist incidents and which are considered to belong to a perpetrator.

- alerts of children at risk of parental abduction, and alerts on children and vulnerable adults who need to be prevented from travelling for their own protection (e.g. when travel may lead to a risk of forced marriage, female genital mutilation, trafficking in human beings).

In the case of children, these alerts and the corresponding procedures should serve the best interests of the child. Such decisions shall be made immediately and not later than 12 hours after the child was located, in consultation with relevant child protection authorities, as appropriate.

The Regulation also permits the introduction of alerts concerning objects for seizure or as evidence in criminal proceedings, such as forged documents and high value objects, as well as computer equipment.

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. Therefore, 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. If available, all relevant data, in particular the first name of the person concerned, must be inserted when creating an alert.

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.

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.

ENTRY INTO FORCE: 27.12.2018.

By 28.12.2021, the Commission will 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.