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

2016/0408(COD) - 10/11/2017 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Carlos COELHO (EPP, PT) 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 committee recommended that Parliament's position adopted in first reading following the ordinary legislative procedure should amend the Commission proposal as follows:

System architecture: the Commission's proposal requires all Member States to have a national copy containing a complete or partial copy of the SIS database as well as a backup N.SIS. Given the risk to data security, Members believe that **Member States should not be required to have a national copy** in order to ensure the availability of the system. As an additional means of ensuring the uninterrupted availability of the SIS, Members proposed that a **back-up communication infrastructure** be developed and used in case of failure of the main communication infrastructure. In particular, the "CS-CIS" (containing the SIS database) or its backup version **should contain an additional copy of the SIS database and be used simultaneously in active operation.**

The CS-SIS and its back-up version should be installed at the technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (the "Eu-LISA agency").

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.

The SIRENE Bureaux shall substantially reply to a request for supplementary information not later than **six hours** after the receipt of the request. In case of alerts for terrorist offences and in cases of alerts concerning, the SIRENE Bureaux shall act immediately.

To further increase the quality of data in SIS, the Agency should also offer **training on the use of SIS** to national training bodies and, insofar as possible, to SIRENE staff and to end-users.

Access to the system: the Commission proposal provides for increased access opportunities for a range of European agencies such as Europol, Eurojust, and the European Border and Coast Guard Agency. The amendments introduced aim to clarify, with regard to the existing mandates of the different agencies, the circumstances in which it is possible to access the SIS data. It is also proposed to strengthen the safeguards in this respect, whether in terms of prior training or logging or oversight, indicating in particular, the date and time of the data processing activity, the type of data processed and the name of the person responsible for data processing.

Data security: Members specified that each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, that: (i) deny unauthorised persons access to data-processing equipment and facilities used for processing personal data; (ii) prevent the unauthorised processing of data in SIS and any unauthorised modification or

erasure of data processed in SIS; (iii) ensure that the installed system may, in case of interruption, be restored; (iv) ensure that faults are reported and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning.

In order to prevent the piracy of SIS by an external service provider, Members proposed that Member States cooperating with external contractors on any SIS-related tasks **closely monitor contractors' activities** to ensure compliance with all provisions of the Regulation, including in particular security, confidentiality and data protection.

Data protection: access to the system should be subject to all the legal provisions applicable to national data protection authorities and to the possibility for the supervisory authorities to verify the correct application of the legal provisions, in particular through the evaluation mechanism of Schengen introduced by Council Regulation (EU) No 1053/2013.

Members proposed a series of amendments that mainly aim to clarify what the applicable rules are. In addition, a number of provisions are strengthened and **brought further in line with EU data protection framework.**

According to the amended text, any introduction and use in the SIS of **photographs, facial images and dactyloscopic data** should (i) remain within the limits of what is strictly necessary to achieve 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 relevant provisions on data protection laid down in the SIS legal instruments, Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council.

Data entered in the SIS **should not reveal sensitive information** about the person, such as ethnicity, religion, disability, gender or sexual orientation.

Alerts on refusal of entry and stay: an alert for the purpose of refusing entry and stay shall be issued **after a national decision** and only:

- if 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 three years**;
- if there are serious grounds for believing that a third-country national has **committed a serious crime or terrorist offence** or there is evidence that a third-country national intends to commit such an offence in the territory of a Member State.

The Member State shall then take an administrative or judicial decision if it concludes, after an individual assessment, that the third-country national poses a threat to public policy or public security or national security.

Only then could the Member State issue the alert for non-admission.

Consultation using biometric data: Members pointed out that **fingerprint data** stored in the SIS should only be used for identification purposes if the identity of the person cannot be established by alphanumeric data (name, first name, date of birth). To this end, the central SIS should contain an automated fingerprint identification system.

Retention period of alerts: The time limit for reviewing personal alerts should be **three years maximum.** As a general principle, alerts should be automatically deleted from the SIS after three years.

Entry into force of the new provisions: in order to avoid long delays, as was the case with the SIS II legal framework, Members proposed that the new legal framework be implemented **one year** after its entry into force.