Second generation Schengen Information System (SIS II): establishment, operation and use

2005/0103(CNS) - 05/10/2006 - ${summary.subTitle}

The committee adopted the report by Carlos COELHO (EPP-ED, PT) incorporating a series of compromise proposals agreed with the Council (under the consultation procedure) on the proposed decision on the establishment, operation and use of the second generation Schengen Information System (SIS II). The proposal was part of a package of legislation defining the legal basis for SIS II on which the committee was seeking to negotiate an agreement with the Council so that the new Member States could be included as soon as possible in the Schengen Information System (see COD/2005/0106 and COD/2005/0104). Given the different policy areas involved and the cross-pillar nature of the SIS, the Commission had to table three legislative proposals: two EC regulations and one third pillar EU decision. The key proposals for the decision were as follows:

- a Management Authority, funded by the EU budget, will be responsible for managing the operation of the SIS II central data base. The Management Authority's personal data processing activities will be monitored by the European Data Protection Supervisor, who will be required to ensure that they are audited to international standards at least every four years. During a transitional period before this authority starts work the Commission will be responsible for the management of the central SIS II. It may delegate the management to national public bodies in two different countries. The European Parliament and the Council must be regularly informed about the conditions and the scope of that delegation;

- personal data processing at national level would be audited by national supervisory authorities, but in cooperation with the European Data Protection Supervisor so as to ensure coordinated supervision;

- each Member State would be responsible for setting up and maintaining a national data system that can communicate with the central SIS II and would have to designate an authority for that purpose. It would also have to take steps necessary to protect personal data;

- with regard to biometrics, photographs and fingerprints may only be entered in SIS II following a special quality check to ascertain the fulfilment of a minimum data quality standard. A search with biometrics should be excluded at the initial stage of the system and will be possible only when that is technically viable. Before this functionality is implemented in SIS II, the Commission will have to report to Parliament on the availability and readiness of the required technology;

- a Member State may create a link between alerts only when there is a clear operational need;

- with regard to data retention periods, alerts on objects for discreet checks or specific checks shall be kept for a maximum of five years, and alerts on objects for seizure or use as evidence in criminal proceedings shall be kept for a maximum of ten years. These conservation periods may be extended should this prove necessary for the purposes for which the alert was issued;

- data processed in the SIS II in application of the Decision shall not be transferred or made available to a third country or to an international organisation. By way of derogation, certain passport details may be exchanged with members of Interpol by establishing a connection between the SIS II and the Interpol database on stolen or missing travel documents, subject to the conclusion of an Agreement between Interpol and the EU;

- in view of the importance of transparency and communication to the public, the Commission and the National Supervisory Authorities shall organise a campaign to inform the public about the objectives, the data stored, the authorities with access and the rights of persons. Such campaigns will have to be repeated regularly and Member States will also have to inform their citizens in general about the SIS II.