Statewatch briefing paper

Schengen Information System (SIS) II: Policing and Criminal Law Decision

Background

On October 5, 2006, the Justice and Home Affairs (JHA) Council, meeting as a 'Mixed Committee' with Schengen associates Norway, Iceland and Switzerland, agreed on the text of a third pillar Decision establishing the second version of the Schengen Information System (SIS II), as regards policing and criminal law. On the same day, the civil liberties committee of the European Parliament (EP) voted in favour of the same text, with the exception of a provision concerning the access of security services to the SIS II database.

The Decision is one of a package of three measures to establish the SIS II, which were proposed by the Commission in May 2005 (COM (2005) 230, 236 and 237). It deals with the issue of the use of the SIS for policing and criminal law purposes, in particular the use of the SIS for the transmission of 'alerts' concerning extradition (including the European arrest warrant), missing persons, wanted persons, surveillance of persons and objects, and missing objects.

The parallel proposals are a Regulation which will regulate the application of the SIS as regards immigration, and another Regulation which will govern access SIS data on stolen vehicles by vehicle registration authorities. The Council and the EP also agreed on these parallel measures on October 5, except (again) for the issue of security agencies' access to data.

The EP plenary is due to vote on the SIS II texts on Monday 23 October, and it remains to be seen whether the EP and the Council will agree to resolve the remaining point of difference between them. If they can, then the two Regulations will be adopted finally pursuant to the 'co-decision' procedure (which requires the EP and the Council to fully agree on the text of legislation), and the third pillar Decision will be adopted finally according to the consultation procedure (which, in this case, also requires a unanimous vote by Member States).

The UK and Ireland are participating in the third pillar Decision, as they have agreed to participate in the relevant provisions of the Schengen rules.

A second version of the SIS was argued to be necessary for technical reasons, as the current version of the SIS cannot accommodate the EU's new Member States. This was also, in the view of the Member States, an opportunity to review issues such as the categories of data to be included in the system and the grounds for listing data, including personal data, in the SIS.

During the negotiations of this proposal, the Austrian Council Presidency in the first half of 2006 sought to drop most of the changes to the existing Schengen Convention rules that had been proposed by the Commission. The final text, agreed under the current Finnish Presidency, is instead closer to the Commission's proposal on a number of issues, due largely to the joint-decision making power of the EP over the parallel immigration Regulation, which is nearly identical to the third pillar Decision as regards the basic rules on the management and operations of SIS II and the data protection rules.

Articles 1 to 14D of the Regulation is effectively identical to Articles 1 to 14AD of the Decision (the basic rules). So are Article 17 of the Regulation and Article 37 of the Decision (the authorities with the right of access to alerts). Article 20 of the Regulation and Article 38 of the Decision, concerning the conservation period of alerts, are identical except for a special provision requiring alerts on surveillance of persons to be reviewed annually. The general data processing rules (Chapter IX of the Decision, Articles 40-48AA; Chapter V of the Regulation, Articles 21-27AA) are identical, except for a different rule about further processing of data (Article 21(4) of the Regulation, Article 40(4) of the Decision) and the possibility to agree a treaty with Interpol on the exchange of passport data (Article 48AA of the Decision). As for the data protection rules (Chapter X of the Decision, Articles 48A-53C; Chapter VI of the Regulation, Articles 27A-31C), the Decision (unlike the Regulation) refers to the application of the Council of Europe data protection Convention (Article 49), and the Regulation (unlike the Decision) contains a right of information (Article 29).

The rules on liability and sanctions are also identical (Chapter XI of the Decision, Articles 54-55; Chapter VII of the Regulation, Articles 32-33), as are the final provisions (Chapter XIII of the Decision, Articles 59-65; Chapter VIII of the Regulation, Articles 34-39).

The following summary looks at the main features of the text of the Decision agreed by the Council, and compares them to the *status quo* (the current provisions of the Schengen Convention concerning SIS II) and to the Commission's proposal. This discussion refers to the parallel Statewatch summary concerning the SIS II Regulation where relevant.

Management of SIS II

As discussed in the parallel Statewatch summary, the SIS is currently managed by France; the Commission had proposed to take over the management of SIS II itself, but this was rejected by Member States. So the agreed text provides that in the

short term, the Commission will nominally be designated as the manager of SIS II, but in practice the Commission will in fact delegate this management to France and Austria (where the backup site of the SIS II data will be located), who will nonetheless be held accountable in accordance with EC rules (Article 12 of the agreed text, and the Joint Declaration on Article 12). In the longer term, an Agency will be established to manage SIS II.

Categories of data

Currently the SIS contains only a few lines of 'alphanumeric' data (letters and numbers). Further data ('supplementary information') is exchanged between Member States after a 'hit' in the SIS (ie a check on a person in police custody reveals that another Member State has apparently issued an alert for extradition for that person). This is known as the 'Sirene' system.

The main change here is that 'biometric' data (photographs and fingerprints) will be included in the SIS. The EP had sought to limit the use of fingerprints, but the Council was insistent on this point (Article 14A). However, the Regulation does provide that biometric data will only be entered following a 'special quality check' in order to ensure data quality (Article 14C(a)). The specifics of this quality check will be established by the Commission pursuant to a 'comitology' procedure, which means that the Commission text must be approved by a 'qualified majority' of Member States' representatives (whose votes will be weighted in the same way as for qualified majority voting in the Council; see Article 61 of the Decision). Initially, biometric data will only be used to 'confirm the identity' of a person whose name has been found in the SIS following an alphanumeric search (likely meaning that his or her name matches a name in the SIS; see Article 14C(b) of the Decision).

But later biometrics will be used to 'identify' persons 'as soon as technically possible' (Article 14C(c)). This will entail a 'one to many' search (comparing one set of biometric data to much or all of the biometric data in the database), which is technically far less reliable than a 'one-to-one' search (which only compares one set of biometric data to the biometric data registered, for example, to the same name). There will be no further vote before this important functionality is put into practice.

Grounds for an SIS listing

The current grounds for listing a person or an object in the SIS in pursuit of a criminal law or policing objective are set out in Articles 95 and 97-100 of the present Schengen Convention. These grounds, as mentioned above, are extradition, missing persons, wanted persons, surveillance of persons and objects, and missing objects. All of these grounds have in principle been retained in the agreed Decision, with no new grounds added.

However, certain changes have been made to these grounds. First of all, the extradition provisions (Chapter IV of the Decision; Articles 15-22) now also refer to the European Arrest Warrant (EAW), and to agreements with non-EU countries which also establish a system similar to the EAW. So far, there is only one such agreement, between the EU and Norway and Iceland; it is not yet in force.

Where an EAW is issued, the Decision provides for a copy of the EAW to be entered into the SIS, and information on the warrant to be communicated via the SIRENE system (Articles 17 and 17A). The information to be provided through the SIRENE system as regards simple extradition requests is the same as under the current rules (Article 95(2) of the Schengen Convention; Article 17B of the Decision), with the addition of 'any other' information which could be 'useful' or 'necessary'. The current provisions requiring a prior check with requested States before an alert is issued, and stating that there is no obligation to arrest nationals, have been dropped in the Decision (compare Article 95(1) and (6) of the Schengen Convention to Article 22 of the Decision).

The provisions on missing persons (Chapter IV of the Decision; Articles 23-26) are essentially the same as Article 97 of the Schengen Convention, with the exception of some clarifications concerning the information which can be entered and the action to be taken following a 'hit' (it will be possible to tell the people who reported a missed person that the latter person has been found).

As for the provisions on wanted persons (Chapter IV of the Decision; Articles 27-30), the only change from the current Schengen provisions is that the information to be transmitted following a 'hit' to the State which issued the alert should be transmitted via the SIRENE system.

The provisions on surveillance of persons and objects (Chapter IV of the Decision; Articles 31-34) have been amended to set out a lower threshold for checks and surveillance of persons for law enforcement purposes. The current rules (Article 99 of the Schengen Convention) provide for checks where there is 'clear evidence' that a person is committing or intends to commit 'numerous and extremely serious' criminal offences, or where there is reason to suppose that this person will commit 'extremely serious' criminal offences in future. But Article 31 of the Decision lowers the threshold for issuing an alert to cases of a 'clear indication' of commission or intention to commit 'serious' criminal offences, referring in particular to the crime subject to 'fast-track' procedures pursuant to the Framework Decision establishing the European Arrest Warrant, or where there is reason to suppose that the person will commit 'serious' offences in future. On the other hand, the provisions on the issue of alerts by security services remain the same as the current rules (Article 99(3) of the Schengen Convention), as amended in 2005 (OJ 2005 L 68). A new provision sets out the circumstances in which an alert can be issued regarding surveillance of an object (Article 31(3a) of the Decision).

As regards missing objects (Chapter IV of the Decision; Articles 35-36), the Decision amends the current rules in Article 100(3) of the Schengen Convention (as

amended by the Council in 2005: OJ 2005 L 68) to provide that data on motor vehicles, trailers and firearms can be included in the SIS even if those objects have *not* been lost or stolen.

Finally, the existing rules on 'flagging' alerts, to prevent the execution of action based upon them, have been amended. These rules apply to extradition and to surveillance of persons. In the case of extradition, the current rules provide that a State may issue a 'flag' preventing an arrest from taking place pursuant to a 'hit' for an extradition alert in the SIS (Articles 95(3) and (4)). The State which issued the alert may ask it to reconsider, but it does not have to. The same applies to alerts for surveillance purposes (see Article 99(6) of the Convention)

In the new Decision, general flagging rules are set out in Article 14B. It will still be allowed for alerts on extradition (including for the European Arrest Warrant) and for surveillance. It will also be possible to flag alerts on missing persons. The discretion for Member States to flag an alert will be wider, as flags can be added when execution of an alert would be 'incompatible with [a Member State's] national law, its international obligations or essential national interests'. In place of the previous rules that a flag should normally be deleted after 24 hours unless the flagging State refuses to give effect to an alert for legal reasons or reasons of expediency, the general rule will apply that a Member State which issued the alert may request another Member State to take action on it in 'particularly urgent and serious cases'; but this does not amount to an obligation for the requested State to take this action.

Article 14C of the Decision sets out particular provisions on the European Arrest Warrant, allowing that flags may be added to alerts either where execution of an EAW has been refused because a judicial authority has refused to execute a warrant due to a ground for non-execution, or (in advance of a decision on non-execution) where it is obvious that execution will have to be refused. A Council Declaration states that this issue may need to be revisited in future, and calls for a report on this issue by the end of 2007.

Access by authorities

Article 37 of the Decision retains the wording of the existing Schengen Convention (Article 101 of the Convention), which gives broad access to the SIS to law enforcement bodies, including also judicial bodies following the amendments to the current SIS rules adopted in 2005 (OJ 2005 L 68). The final Council version of Article 17 contains the vague words (intended to refer to access by security services) which the EP has not (yet) consented to.

In the 2005 amendments to the current SIS rules, the Council had also amended the Schengen Convention to allow for access to SIS data by the EU's policing agency, Europol, and the EU prosecutors' agency, Eurojust (new Articles 101A and 101B). These provisions were applied with effect from 1 October 2006. The agreed Decision makes no changes to the current rules applicable to Europol

access to SIS data (Article 37A), but it will amend the rules concerning Eurojust. Eurojust will in future have access to data concerning not only extradition and wanted persons (as at present), but also access to data concerning missing persons and missing objects (Article 37B of the Decision).

Data protection

As noted above, the Decision contains the same provisions as the SIS immigration Regulation concerning data protection (see the separate summary), with the absence of a right to information and the addition of provisions requiring the application of the Council of Europe's data protection Convention and limiting the exchange of data to third parties other than Interpol as regards passport data.

Compared to the existing rules, the Schengen Convention already requires the Member States to apply the Council of Europe data protection Convention (Article 117(1) of the Convention). But the Convention currently does not contain any provisions concerning a right to information for data subjects, and it is silent on the issue of transmission of SIS data to third parties.

It should be noted that the proposed EU Framework Decision on data protection will apply to the SIS II Decision, as set out in recital 20a of the preamble to the Decision. This will also follow from Article 34(1) of the proposed Framework Decision, which states that the Framework Decision will replace all references to the Council of Europe data protection Convention that appear in any EU measures. It should be noted that the rules in the Framework Decision (in its current form; it is still under negotiation in the Council) set higher standards than the SIS II Decision in some respects (such as a right to information), but lower standards in others (such as the transfer of data to third parties).

Final provisions

As with the immigration Regulation (see separate summary), SIS II will begin operations once the Council (made up of Member States currently fully participating in Schengen) decides unanimously (Article 65(1a)). As noted in the separate summary, this is now planned for 2008.

There are detailed provisions on monitoring and statistics (Article 59), going well beyond the current requirements for SIS public accountability.

The Commission will have power to adopt implementing measures, subject to Member States' control in a 'comitology' committee (Article 61); it has some of these powers already as regards amendment of the 'Sirene manual' (which governs the transmission of further data between Member States following an SIS 'hit'). The Commission had actually proposed that for some matters, Member State representatives would only have an *advisory* role, unable to block the

Commission's proposed measures (Article 60 of the Commission proposal), but this was rejected by the Member States.

The power to adopt implementing measures will apply to the following:

a) the adoption of the Sirene Manual (Article 8(3a));
b) technical compliance between the national and central databases (Article 9(1));
c) 'technical rules' concerning 'entering, updating, deleting and searching the data' (Article 14a(3a));
d) the specifications for a quality check before the uploading of biometric data (Article 14c(a));
e) 'technical rules' concerning 'entering, updating, deleting and searching the data' concerning missing objects (Article 35(3));
f) 'technical rules' concerning 'entering, updating and deleting the data' concerning misused identity (Article 44(3)); and
g) 'technical rules' for linking alerts (Article 46(4a)).

This list is identical to the list applicable to the immigration Regulation, except for point (e).

As with the immigration Regulation, existing SIS data will have to be subject to the new rules in the Regulation three years after the SIS II begins operations (Article 64); if SIS II is operational as planned in 2008, this means that the existing data will have to be amended by 2011. However, during this three-year period, any type of amendment made to a pre-existing alert must comply with the Regulation, and a Member State must 'examine the compatibility' of an alert with the Regulation in the event of a 'hit' (ie where a check in the SIS reveals that a person is wanted for extradition, or surrender pursuant to a European arrest warrant). But in the latter case, this examination of compatibility will not affect the action to be taken (ie Member States will in principle still have to execute the arrest warrant, unless there is a ground for non-execution of the warrant).

Conclusions

The new Decision will differ from the current Schengen rules as regards the inclusion of biometric data. The rules on types of alerts will also be amended to include copies of European Arrest Warrants and connected data, and a lower threshold to issue alerts relating to surveillance. Access to SIS data would also be widened for Eurojust and (if the Council's text is accepted) security agencies. The Decision will also alter the current rules on data protection and (ultimately, following the creation of an agency) management of the system.

Statewatch, October 2006

References:

Current Schengen Convention: see Articles 92-119
COM (2005) 230: proposed third pillar Decision to establish SIS II
COM (2005) 236: proposed Regulation establishing SIS II as regards immigration
Draft opinion of the European Parliament LIBE committee
Council doc. 5710/7/06: agreed text of SIS II Decision

Full-text documents available on:
http://www.statewatch.org/news/2006/oct/11eu-sis-II-sources.htm