OPINION
ON
THE DEVELOPMENT OF SIS II

1 Introduction

In an attempt to ensure that the second-generation Schengen information system − SIS II − complies with the highest standards of data protection, the Joint Supervisory Authority (JSA) has sought to influence the development of the system from the outset.

Although the Council, in its conclusions of 5 and 6 June 2003, set out some general requirements for the new system, there has not been a final decision regarding the exact content and functionalities that are to be incorporated − nor even, crucially, on the exact purpose of this second-generation system.[1]

This opinion considers how the original purpose for which the SIS was created has evolved and examines the various proposals for the SIS II, reflecting on how these might change the character of the system. Finally, the opinion sets out the reasons behind the JSA's view that a decision on what it is that the new system is intended to do ought to be taken as soon as possible.

The JSA will continue to monitor the development of the SIS II, providing more detailed guidance once specific proposals for the system have been confirmed.

2 The Schengen Information System

2.1 Background

The SIS was originally created as one of a number of compensatory measures to allow for the free movement of persons. The system itself provided a means of carrying out border checks and other police and customs checks.

As the relevant authorities had to be able to perform these checks quickly, the system took shape as a hit/no hit system. In practice this meant that when a person was the subject of a control, a search of the SIS would reveal whether an alert had been entered on the person in question and, if so, the immediate action to be taken. The SIS was intended to process only those data necessary for this purpose − any additional information had to be obtained via the SIRENE bureaux.

Responsibility for processing data in the SIS and provisions to safeguard the rights of individuals were set out in the Schengen Convention. The latest figures indicate that the SIS currently holds information on around one million people.

---

[1] Reference is made throughout this document to the conclusions of the Council; in each instance this refers to the conclusions of the meeting of the European Council on Justice and Home Affairs held in Luxembourg on 5 and 6 June 2003

2.2 Changing context

In 2003 the Council concluded the following:

"The SIS is a hit/no hit system allowing for information exchange with a view to policing the free movement of persons as well as maintaining public security, and in particular assisting national authorities in the fight against trans-national crime, in the context of the EU objective to maintain and develop the Union as an area of freedom, security and justice."

This is arguably a wider definition of the system than that set out under Article 93 of the Schengen Convention, and it serves to indicate the context in which the SIS has come to be viewed since the Schengen *acquis* was incorporated into the legal and institutional framework of the European Union.

Increased co-operation between national law enforcement agencies and the creation of new organisations such as Europol led to a situation in which the information held in the SIS was viewed as a valuable resource in the fight against crime and terrorism.

A new Schengen information system was proposed in order to cope with EU enlargement, and it was thought that this new system would be able to take advantage of new technologies while also taking account of other developments in the field of justice and home affairs. It is in this context and with these general objectives in mind that the proposals for the SIS II have been developed.

3 SIS II

3.1 Developing a new system

It might be said that there are three strands to the development of a new information system of this kind: the political decision-making process, which should establish what it is the system is intended to do and how it will do this; the legal framework providing a legal basis, specifying the purpose of the system and setting out rules regarding access and so on; and the technical development of the system itself.

Firm proposals on the purpose and functionalities of the SIS II were originally scheduled to come out of the Council meeting of June 2003 but, as the European Parliament noted in its recommendation, "the Council remains undecided on concrete questions such as which new categories of objects or persons to include".[2]

This absence of clear guidance has resulted in a situation where the Commission has had no option but to propose developing the new system to be as flexible as possible. Consequently, the development of the system is being driven by the changing demands of

[2] European Parliament recommendation to the Council on the second-generation Schengen information system (SIS II), 20 November 2003

justice and home affairs in the EU rather than by a stated purpose laid down in a legal framework; if this continues the character of the system could change completely, with the SIS II evolving into a multipurpose investigative and administrative tool. It would be worrying if the development of the SIS II were to continue on such a piecemeal basis, as the lack of transparency inherent in this approach makes it difficult to assess the resulting changes in the system's character.

3.2 SIS II − A flexible tool

"It has been clear from the earliest conception of SIS II that this system should be a flexible tool, . . . able to adapt to changed circumstances and fulfil, within a reasonable time and without major additional costs and efforts, user requests made during its lifecycle."

The above extract from the Council conclusions of June 2003 highlights a defining feature in the development of the SIS II; indeed, in its most recent Communication the Commission listed "flexibility" as one of the key requirements of the new system, stating that "SIS II should have the potential to handle a significantly larger number of data and, once operational, to be extended to cope with new information types, new objects and further new functions, which are under discussion in the Council framework." [3]

This requirement to construct a flexible system of undefined character poses several problems.

First there is the concern that a flexible system would be more likely to result in "function creep", with demands from a range of agencies and organisations leading to a situation where the information held in the system is used for purposes for which it was not originally intended.

Secondly, it is difficult to see how there can be a proper assessment of the potential implications of the SIS II when its development is to be so flexible that it is unclear what form the system will ultimately take. The creation of such a flexible system without any restrictions must also make it more difficult for those developing the system to take account of the principle of proportionality, which ought to be a guiding principle in any project of this nature.

As the system develops, with new users and additional categories of information, the legal framework will have to evolve accordingly, not least because the safeguards currently in place to protect the rights of individuals were designed to cope only with the SIS as originally conceived. The JSA would suggest that, as a first step, there should be a privacy impact assessment to determine the impact that the SIS II and its various new functionalities might have on the rights of individuals; such an assessment might then form a basis from which to devise a new legal framework.

---

[3] Communication from the Commission to the Council and the European Parliament: Development of the Schengen Information System II and possible synergies with a future Visa Information System, 11 December 2003

4 SIS II − Proposed changes to the system

4.1 Access to the system

The demands made of the SIS in recent years have reflected EU developments in the fight against crime and terrorism. There was, for example, a Spanish initiative which sought to grant Europol and Eurojust access to the SIS.[4] Allowing such organisations access to the system will have consequences for the character of the SIS II, as the information obtained from the system is more likely to be put to operational use by these organisations − by Joint Investigation Teams at Europol, for example. The JSA remains of the view that the tasks for which access is granted must be in accordance with those articles of the Schengen Convention that deal with access to and use of information held in the system.

Allowing outside bodies access to the SIS can even result in a complete change in the purpose for which the information in the system is used. In a recent opinion on a Commission proposal to grant vehicle registration authorities access to the SIS, the JSA noted that such a move would mark a departure from the original purposes of the system, as implementing the proposal would result in the SIS being used to support the EU's common transport policy.

Nonetheless, the trend towards granting access to a wider range of bodies looks set to continue: the Council concluded that new authorities must be able to access the SIS II, even if this meant the possibility of "partial access or access with a purpose different from the original one set in the alerts".

The JSA understands that increased co-operation between law enforcement agencies is essential in order to improve security throughout Europe and, to this end, allowing other organisations to access the information held in the SIS II might prove to be appropriate in certain cases. However, access to the system should only be permitted where it is necessary and proportionate, not simply because it is possible. For this reason, the JSA is of the view that there ought to be clarification of the specific tasks for which Europol and Eurojust (and any other organisations) require access to the SIS II; and the legislative overhaul that should accompany the development of the new system would seem to provide the ideal opportunity to ensure that such tasks and relationships are laid down in a clear legal framework.

This legal framework should place restrictions on what organisations can do with information obtained from the system, and it is important to ensure that organisations granted access to the SIS II are required to comply with the same standard of data protection found in the Schengen Convention and other relevant legislation, such as the 1981 Council of Europe Convention on data protection.

The piecemeal approach to deciding which authorities should have access to the SIS is of continuing concern to the JSA. Despite the Council conclusions of June 2003 and the Commission's intention to design the new system to be as flexible as possible, the JSA would support the recommendation of the European Parliament that "data should be used

[4] This initiative culminated in the adoption of Council Regulation (EC) No 871/2004 on 29 April 2004

only for purposes expressly stated well in advance". In its recommendations the Parliament objected to any derogations from this principle "such as those expressed in the Council conclusions of 5 and 6 June 2003 calling for further examination of the 'possibility for some authorities to use the SIS data for purposes other than those for which they were originally introduced in the SIS'."

If it is to be possible to grant access to new organisations once the SIS II is in operation, there should be clear criteria on which to base such decisions. These criteria ought to be set out in the legislation and should take account of whether, for example, access will be granted to private organisations as well as public bodies.

4.2 Information in the system

4.2.1 Additional categories of information

It seems likely that the pressure to add new categories of information to the system will increase, particularly as the proposal to construct the SIS II as a flexible system will make it easier to add more categories in future. There have already been developments in this area: the Council Framework Decision establishing a European arrest warrant provides for the information in the new warrant to be processed in the SIS. The addition of new categories of information could lead to the SIS II duplicating other EU information systems such as the Europol information system or the customs information system − a development which might have implications for the standard of data protection.

The JSA is of the view that there should be clear criteria for deciding what can be held in the SIS II and, once again, the purpose of the system has to provide a starting point for such decisions.

4.2.2 New types of information: Biometric identifiers

There are plans to introduce new types of information and there has been particular interest in biometric data.

It is argued that it is necessary for the SIS II to hold unique identifiers to enable competent national authorities to resolve problems concerning a person's identity and the Council has concluded that the SIS II should allow for "the storage, transfer and possible querying of biometric data, especially photographs and fingerprints."

The Communication from the Commission (December 2003) provides examples of situations in which the use of biometric identifiers would be of assistance. One such example is where the authorities have apprehended a person in possession of false documents. At the moment it would not be possible, using only the information held in the SIS, to establish whether an alert had been entered on that person under another name. However, if the system also stored biometric identifiers, such as fingerprints, it might be possible to compare the fingerprints of the individual in question against all those held in the system. Thus, users would be able to establish whether or not an alert had been entered on that person under another name.

In another example of a case where access to biometric identifiers would be useful, the Commission cited a situation where the system registers a hit but the person in question claims that the alert concerns another person ("false" hits are apparently quite frequent when common names are involved). It is argued that such cases could be resolved quickly if the authorities were able to compare the biometric identifier of the person in question against the identifier that features alongside the alert in the system. This would allow the authorities to establish whether that person was in fact the person on whom the alert had been entered.

These examples illustrate the two fields of application available when building a biometric facility into an information system. The first option, where the user runs a query searching all the biometric identifiers in the system for a match (a one-to-many comparison), is known as the "identification" system; and the second option, where the biometric identifier of a particular person is checked against a specific alert in the system to establish whether or not they are that person (a one-to-one comparison) is known as the "verification" system.

The reliability of these two systems differs − as do the uses to which they can be put − but, whichever is chosen, this is yet another example of a decision that has to be taken with the system's purpose as a starting point, applying a test of proportionality.

4.2.3 New types of information: Some basic safeguards

The inclusion of biometric data involves a variety of practical problems that have yet to be resolved (the way in which biometric identifiers will be collected, for example) and until detailed plans have been proposed it is difficult to know what additional safeguards might be needed, but at the very least the inclusion of biometric data would require a clear legal framework stipulating in exactly what circumstances and for what purposes searches of biometric data may be carried out. This is particularly important given that the inclusion of biometric data makes the prospect of function creep more likely; with organisations, and the law enforcement community in particular, taking advantage of the proposed flexibility of the SIS II to request access to biometric data for a range of purposes.

This risk would be even greater if the biometric data were to be held in the national sections as well as the central section of the SIS II, as national law enforcement agencies might then have more opportunity to use these data for purposes outside the scope of the Schengen Convention.

In order to safeguard against this, access to new categories of information should be logged, with regular audits of the system to ensure that information is only being accessed for a legitimate purpose and by those entitled to access it. Furthermore, rules on the retention of new types of information must make it clear that such information can be held only for as long as necessary for a specified purpose.

4.3 New technical functions

One of the reasons for developing the SIS II was to take advantage of new technologies by introducing new functionalities. It is proposed that the SIS II should allow the

"interlinking" of alerts in the system in an attempt to improve efficiency. The JSA has stated that a legal framework must precede such a move and, in a past opinion, the JSA warned that the interlinking of alerts might allow users to access information to which they are not entitled; the JSA therefore welcomes the Council's statement (included in its conclusions) that there should be safeguards in place to ensure that the interlinking of alerts "does not change the existing access rights to the different categories of alerts".

Nonetheless, the interlinking of alerts is an example of a functionality that could lead to a change in the character of the system from a reporting system to an investigative system.

5 Control of SIS II

The proposed architecture of the new system raises questions regarding control and supervision. If the system becomes increasingly centralised, how will supervision have to evolve? It may be that the JSA will need more powers in order to adapt to any changes in the architecture of the system.

The Commission's Communication said that Contracting Parties could choose either to maintain a national database or to have only a national interface and query the central system directly. What might the implications of this change be?

At present, the Schengen Convention provides national data protection authorities with the power to supervise their respective national sections of the system. If the national sections were to be replaced by an interface, there would be consequences for national supervision and the legal powers afforded to national authorities might have to change accordingly. There would also be a need to ensure that all the relevant supervisory authorities have sufficient resources to carry out effective supervision of the system. In any case, future discussion of the control and supervision of the SIS II ought to involve the national data protection authorities, as well as the JSA and the newly-appointed European Data Protection Supervisor.

6 Conclusion

Although it might not be the intention to change the character of the SIS from a hit/no hit system of control, the JSA is of the view that the addition of new functionalities (such as the interlinking of alerts), the inclusion of new types of information, and the trend towards allowing a wider range of bodies access to the system − when combined with the proposed flexibility of the new system − may well result in a *de facto* change in the character of the system, with the SIS II evolving into an investigative tool.

This is not a new idea: in 2001 the Commission itself said the following:

"The Commission would like to stress the importance of making progress in defining the functions of the SIS. In particular some of the proposals currently under discussion would

fundamentally change the purpose of the SIS, transforming it from a reporting system to a reporting and investigating system." [5]

There are good reasons why we should be concerned about such a development. First there is the possibility that as the SIS II incorporates new data categories it will duplicate existing EU information systems. Secondly, rules on data protection ought to be updated to ensure that the new system with its different capabilities does not impinge on the rights of individuals − and these rules are always going to be a step behind if there are to be no checks on the way in which the system develops. It is also important that the SIS II should be developed in accordance with the principle of proportionality; that is to say that the functionalities and data categories that the SIS II incorporates must not go beyond what is necessary to achieve the purposes of the system. However, the purposes must first be established before this can be tested.

The JSA would reiterate that before the legal and technical questions can be resolved there has to be a political decision on what the SIS II is intended to do, and the functionalities and data categories that it should incorporate in order to do this ought to be defined in detail.

Furthermore, there would not yet appear to be any initiatives within the Council to start work on devising a new legal framework for the SIS II and, for the reasons set out in this opinion, the JSA would urge that work on this should begin as soon as possible. The findings of a privacy impact assessment would prove useful when drawing up this legal framework and, as well as examining any related proposals such as the proposed synergy between the SIS II and a new Visa Information System, an assessment of this kind could consider the supervision of the system and whether additional safeguards are required.

For its part, the JSA is willing to assist wherever possible. Moreover, given the far-reaching implications of the proposals for the SIS II, the JSA would expect to be informed of any further developments at an early stage so that there might be time to prepare guidance which can then be taken into account by decision makers.

Brussels, 19 May 2004

[5] Communication from the Commission to the Council and the European Parliament: Development of the Schengen Information System II, 18 December 2001