

OPINION ON THE PROPOSED LEGAL BASIS FOR SIS II

Chapter I

1. Introduction

The need to develop a new, second-generation Schengen Information System (SIS), as well as the wish to introduce new functions for the SIS have been the subject of discussion for several years.

On 31 May 2005 the Commission presented its proposals for a legal basis for the new Schengen Information System, the SIS II:

- a proposal for a Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II) COM (2005) 230, 2005/0103 (CNS), hereinafter referred to as ‘the Decision’;
- a proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) COM (2005) 236, 2005/0106 (COD), hereinafter referred to as ‘the Regulation’;
- a proposal for a Regulation of the European parliament and of the Council regarding the access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM (2005) 237, 2005/-104 (COD), hereinafter referred to as ‘the vehicle registration Regulation’.

The proposed legal basis for SIS II will be a crucial milestone in the further establishment of an area of freedom, security and justice, including the creation of an area without frontiers. The experience of the past decade, which has seen cooperation between states in the present Schengen Information System, has demonstrated that the legal basis for such a system is not only crucial for facilitating cooperation between states, it also provides the best means of guaranteeing adequate protection of fundamental rights and ensuring effective supervision.

The Schengen Joint Supervisory Authority (the JSA) has followed the development of the SIS II with interest, and has taken a number of initiatives to encourage discussion of the subject – one notable example being a seminar on SIS II, organised by the JSA and held in the European Parliament in October 2003.

Consequently, the JSA very much welcomes the fact that the Vice-President of the European Commission, Mr Franco Frattini, requested the JSA to deliver its opinion on these proposals, as did the Chairman of the Council's Article 36 Committee.

Opinions on this subject are also being drawn up by the European Data Protection Supervisor and the Article 29 Working Party, which advises the Commission on data protection issues in the first pillar.

2. Summary of Conclusions

The SIS is an important example of successful cooperation between European countries, and the second generation of the system, the SIS II, aims to build on this success. The JSA recognizes that considerable work has gone into creating a legal basis for the SIS II, including a set of data protection provisions.

The JSA has the following fundamental concerns, relating to four aspects of the proposals:

i) The application of existing EU data protection laws, together with the present proposals, will result in a situation in which four European legal instruments will apply to the SIS II and the use of SIS II data. With this open-ended legal structure it may sometimes be unclear what is regulated by which instrument. There is also the question whether these instruments will regulate the SIS II comprehensively; for example, it is not clear whether Member States may deviate from these various provisions – and, if so, to what extent. It is in the interest of the participating Member States and the data subjects that the legal basis is clear and comprehensive. In its opinion the JSA shall further explore this subject and present solutions.

ii) It is not clear from the proposals who will be responsible for the SIS II. The proposals set out some responsibilities of the Commission and of Member States, but they do not solve all the problems involved in control. This problem is examined in more detail elsewhere in this opinion.

iii) Another subject that needs close attention is the purpose of the SIS II. The stated objective, combining the quite specific purpose of conducting controls on persons with the much more general purpose of assisting police and judicial cooperation, is a cause for concern. Moreover, the fact that Europol, Eurojust and authorities responsible for vehicle registration will have access to the SIS II further highlights the move towards the development of the SIS II as an investigation tool. The legal basis fails to comply with one of the key principles of data protection; namely, that the purpose of processing must be specified and explicit.

iv) The proposed supervision by the European Data Protection Supervisor (EDPS), his new task, the relation between that task and Regulation 45/2001 describing the powers and duties of the EDPS, and the relation with the national supervisors have not been sufficiently regulated in the present proposals. There ought to be provision for an institutionalised joint role for the national data protection authorities (and the EDPS). The proposed model of supervision currently places too much emphasis on the central processing, which will be minimal.

In this opinion the JSA has addressed these subjects and has made recommendations on several other matters.

3. Structure of the opinion

The existence of different proposals makes it necessary to structure this opinion as follows: Chapter I deals with the legal basis and its implications; Chapter II contains some general remarks on the proposed legal basis. Detailed comments on the Decision can be found under Chapter III, with Chapter IV examining the Regulation. Finally, Chapter V concerns the vehicle registration Regulation.

4. Legal basis

4.1 Relevant data protection framework

The processing of personal data in the SIS, and in the SIS II, must comply with the following principles:

- The right to respect for private and family life guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and reaffirmed by Article 7 of the Charter of Fundamental Rights of the European Union, and the fundamental right to data protection which is enshrined in Article 8 of that Charter.
- The ECHR allows interference with the right to privacy if necessary for the interests referred to in the second paragraph of Article 8 and when justified by those interests; such interference must take account of the principle of proportionality. Article 8 of the Charter of Fundamental Rights expands on this, stipulating that personal data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This legitimate basis has also to fulfil the conditions of proportionality.
- The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) provides more specific principles for data protection also applicable in the Third Pillar. A Recommendation with specific data protection provisions regulating the use of personal data in the police sector was adopted in 1987 by the Committee of Ministers to Member States.¹

In EU legislation harmonized basic rules on data protection are laid down in:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Directive 95/46').
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data ('Regulation 45/2001')

¹ Recommendation No. R (87) 15, of 17 September 1987

Each EU Member State also has to take account of its own national legislation on data protection.

4.2 Proposed legal basis SIS II

Title VI of the Convention of 1990 implementing the Schengen Agreement of 14 June 1985 (further referred to as the Schengen Convention), established the Schengen Information System and set out specific rules for the processing of data. These provisions include a comprehensive overview of the categories of authorities that have access to the SIS and the purpose for the use of the SIS data. This did not change with the integration of the Schengen *acquis* into the legal and institutional framework of the EU in 1999.

The Schengen Convention required the contracting parties to adopt the necessary national provisions in order to achieve a level of protection of personal data at least equal to that resulting from Convention 108 and Recommendation No. R(87) 15.

At present Schengen is governed partly by community law and partly by intergovernmental agreement, which explains the need for the current system of dual supervision shared between the JSA and the European Data Protection Supervisor (the EDPS). This division is repeated in the proposed legal basis for the SIS II, with the Decision based on the Treaty of the European Union and the Regulation based on the Treaty establishing the European Community. Consequently, Directive 95/46 will apply to the processing of personal data that takes place under the Regulation. The Directive will not apply to the processing of personal data under the Decision; instead, this processing will only have to comply with Convention 108 and Recommendation No. R (87) 15. The JSA, among others, has said previously that Convention 108 alone is not sufficient; there is now a need for an instrument guaranteeing a higher level of data protection in the third pillar.² The proposed framework decision on data protection in the third pillar would be one way of resolving this problem.

Although two legal bases exist, the SIS II should be regarded as one system under the operational management of the Commission. Although only part of the processing of personal data in the SIS II falls within the scope of Community law, the Commission's role with relation to the SIS II leads to the application of Regulation 45/2001 in the processing of personal data in application of both the Regulation and the Decision. Recital 21 of the Decision explains that this is done to promote a consistent and homogeneous application of the rules regarding the protection of fundamental rights and freedoms.

As the SIS II may be characterized as a system in which Member States' data will be processed by a central system operated by the Commission, further clarification of the present proposals is required.³ In particular, there is a need for clarification of the following subjects:

- i) The mutual relation between the different legal instruments
- ii) The Controller of the SIS II
- iii) Supervision of the SIS II

² See the Declaration of the Spring Conference of European Data Protection Authorities (and the accompanying position paper on Law Enforcement & Information Exchange in the EU). Krakow, 25-26 April 2005

³ The term 'Member States' when used in this document should be taken to include those non-EU countries that apply the Schengen *acquis*

4.2.1 The mutual relation between the different legal instruments

According to Recital 21 of the Decision and Recital 15 of the Regulation, Regulation 45/2001 is applicable to the processing of personal data carried out by the Commission in application of the Decision and the Regulation, and the principles of Regulation 45/2001 should be supplemented or clarified by the proposed legal basis for the SIS II. Apart from these general rules, other specific legislation such as the Framework Decision on the European Arrest Warrant will have some impact on the SIS II. Application of Regulation 45/2001 seems logical as far as the Commission will be processing personal data. However, the proposal as presented by the Commission creates a situation where Regulation 45/2001 applies in its totality except where there are specific provisions in the Decision and the Regulation. For example, there is a question whether Article 20 of Regulation 45/2001, which sets out exemptions and restrictions, would allow the Commission to restrict the principle that personal data may not be processed in a way incompatible with the purpose of processing in the interest of the prevention, investigation, detection and prosecution of crime. If so, how would that relate to the responsibility that Member States have for the data content of the SIS II? Similarly, Recital 14 of the Regulation states that Member States may adopt legislative measures to provide for exemptions and restrictions by using Article 13 (1) of Directive 95/46. The application of these various legal instruments, supplemented by provisions included in the new proposals, is bound to be a cause of considerable confusion. This situation might be improved if the Commission were to produce some form of vade mecum, listing all the rights that will exist in relation to the SIS II and providing a clear hierarchy of applicable legislation.

In contrast to the present legal basis for the SIS, which contains comprehensive provisions on the processing of data and a strict data protection regime governing the use of personal data, the proposed legal basis for the SIS II seems to be less comprehensive – allowing Member States discretion on crucial matters such as the use of SIS II data.

Taking into account the mixed character of personal data originating from the participating states and the impact of the use of those data for the individual, it is important to have a transparent and comprehensive legal basis for the SIS II.

Both the Decision and the Regulation should thus be viewed as a comprehensive legal instrument for SIS II. This would prevent any discussion on the possibility that the Commission or Member States might deviate from the proposed legal basis using the exemptions available in Regulation 45/2001 and Directive 95/46. The recitals in both the Decision and the Regulation should underline this comprehensive character. The legal instruments for the SIS II should be accompanied by some form of vade mecum which could list all the rights that will exist in relation to the SIS II and provide a clear hierarchy of applicable legislation

4.2.2 The Controller of the SIS II

In order to ensure compliance with data protection principles, it is essential to establish which body is the data controller. Regulation 45/2001, which applies to the Commission when carrying out its tasks in relation to the SIS II, defines the controller as *‘the Community Institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of processing of personal data; where the purposes and means of processing are*

determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act.'

Neither the Decision nor the Regulation designate a controller of the SIS II.

In addition to a controller, a processor may be present. A processor is defined in Regulation 45/2001 as *'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.'*

Responsibility for the processing that takes place in the SIS II is very important, not least because it will in large part determine the nature of supervision required. For example, the nature of the Commission's role will have an impact on whether the focus of supervision should be at national or European level.

According to the Decision and the Regulation, the Commission shall be responsible for the operational management of the SIS II. The description of these responsibilities seems to indicate that the role of the Commission is that of a processor. In that case, the question remains who will be the controller of the SIS II. Since the data to be processed in the SIS II will be first and third pillar data it might be possible to appoint more controllers with different responsibilities such as the Member States and the Commission. The choice of the controller or a combination of controllers should in any case reflect a practical structure ensuring full compliance with all the different responsibilities and tasks of the controller(s). It should be noted that the EDPS will not be competent for activities that go beyond the Commission's role. Given the different responsibilities of the Commission and Member States, the need for consistent and effective control of the SIS II and the practical implementation of the rights of the data subject, a combination of controllers will be more effective. The JSA is of the view that the Commission and Member States will be joint controllers of the system: with the Commission responsible for its specific tasks as described in the proposals, and each Member State having responsibility for the data it processes in the system. The legal basis should make it clear where the division of responsibility between the Commission and Member States lies.

4.2.3 Supervision and Control

Once the Commission has clarified the provisions regarding the controller of the system, it will have to ensure that there is a corresponding model of supervision, with appropriate supervision at national and at EU level. The proposals for supervision of the SIS II ought to take account of work currently being done to draft a framework decision on data protection in the third pillar.

The Schengen Convention provides for a system of data protection supervision which distinguishes between national supervision and supervision of the central SIS unit by the Joint Supervisory Authority. The national supervisory authorities are represented in the JSA. The JSA strongly advocates comprehensive provisions for the SIS II and the further processing of personal data, with clear provisions on supervision and control of the SIS II.

In the proposed legal basis for the SIS II, supervision and control on the national level seem to remain unchanged. The only obvious change is the supervision of the technical architecture of the SIS II as defined in the Decision and the Regulation. As a consequence of the Commission's role, Regulation 45/2001 applies and the European Data Protection Supervisor will monitor the data processing activities of the Commission. Although this seems an obvious solution, this new task for the EDPS raises some questions that need attention.

Both the Decision and the Regulation describe the task of the EDPS as being ‘to monitor that the personal data processing activities of the Commission are carried out in accordance with the Decision and the Regulation’.

It is not clear, however, what the exact scope of such supervision will be. Will it be limited to a ‘simple’ monitoring function, or does the relation between the Decision and the Regulation and Regulation 45/2001 also imply that all the duties and powers of the EDPS are applicable?⁴ If the latter is the case, the designation of the EDPS as supervisor will allow the data subject to lodge a complaint with the EDPS, with the EDPS having the power to impose a ban on processing. This is in addition to the provisions regarding the rights of the individual and the supervision of data processing as referred to in Chapter X of the Decision and Chapter VI of the Regulation.

As the SIS requires Member States to cooperate by sharing personal data, the JSA was set up with emphasis on joint responsibility for the personal data processed in the SIS. For this reason, Article 115 of the Schengen Convention charges the JSA with the following tasks:

- i) Supervising the technical support function of the SIS and checking that the provisions of the Schengen Convention are properly implemented;
- ii) Examining any difficulties of application or interpretation that might arise during the operation of the SIS;
- iii) Studying any problems that may occur with the exercise of independent supervision by national supervisory authorities;
- iv) Studying any problems that may occur in the exercise of the right of access to the system;
- v) Drawing up harmonised proposals for joint solutions to existing problems.

Practice has demonstrated that these tasks are necessary in supervising a joint system like the SIS.⁵ Some of these tasks are closely related to the joint character of the SIS and the role and responsibilities of the Member States, and they will be equally important for supervision of the SIS II. The participation of all national data protection supervisors in the supervision of the SIS indicated the need for a joint approach to supervising a joint system. The proposals for the SIS II legal basis, even in conjunction with Regulation 45/2001, do not provide for all these essential tasks, nor do they provide for a joint approach. For example, in the current proposals there is no provision equivalent to Article 115 (3) of the Schengen Convention, which requires the JSA to examine any difficulties of application or interpretation that might arise during operation of the SIS, to study any problems relating to national supervision or the right of access and, on encountering any problems, to draw up harmonised proposals with a view to finding a joint solution. The proposed model of supervision currently places too much emphasis on the central processing, which will be minimal.

The JSA therefore urges the Council to reflect on the role of the SIS II supervisors, taking the following aspects into account:

⁴ Article 45 and 46 of Regulation 45/2001

⁵ See, for example, the Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System (20 June 2005)

- i) The responsibilities of Member States must be clarified, with clear provisions on the specific supervisory tasks that national supervisors will have in relation to the SIS II.
- ii) The JSA's experience confirms that cooperation plays an important part in coordinating national supervision. The proposal for an annual meeting of national data protection authorities, to be convened by the EDPS, is insufficient, particularly as there is a need for joint supervision of data entered directly in the CS-SIS by Member States. There ought to be a requirement for an institutionalised joint role for national data protection authorities (and the EDPS). Provision for institutionalised joint supervision is particularly important as not all states that apply the Schengen *acquis* are members of the EU.
- iii) Supervision of the SIS II must include all tasks referred to in Article 115 of the Schengen Convention.
- iv) While it is recognised that both the EDPS and the Member States have a supervisory role to perform, their supervisory tasks must be clearly delineated.
- v) An exhaustive list of the duties and powers of the EDPS should be defined in the Decision and the Regulation, taking into account the specific character of the SIS II and the relationship with Member States.

Chapter II

5. General comments on the Decision and Regulation

5.1 Interlinking of alerts

The Council Conclusions of 14 June 2004 on the functional requirements of the SIS II define criteria applying to the developments of links between alerts.⁶ Apart from the criteria regarding the legal basis of alerts and links, the Council concluded that each link should have a clear operational requirement, respect the principle of proportionality and be based on a clearly defined relationship. Furthermore, interlinking must not create new access rights. The existence of a link should not be visible to the users unless they have access rights to view the related alert.

In the past, the JSA has warned that the interlinking of alerts might allow users to access information to which they are not entitled; and, while the JSA welcomes the provision in the Regulation which states that 'links shall not affect the rights to access provided for in this Regulation' (there is a corresponding provision in the Decision), there remains the question whether this provision is sufficient.

Article 46 of the Decision and Article 26 of the Regulation specify the rules for interlinking alerts, stipulating that Member States may create links between alerts in the SIS II in order to 'establish a relationship between two or more alerts'. There are dangers with this proposal, particularly given the number of alerts likely to be held in the system. It is not clear, for example, whether the Regulation will allow Article 15 alerts to be linked only to other Article 15 alerts, or whether links may be made between all other alerts in the system. If the latter is the case, the Regulation should specify when such links might be made – bearing in mind that most of the alerts provided for by the Decision will not be accessible to asylum and immigration authorities.

Another aspect of interlinking is connected to the purpose of the SIS II. If the system's purpose is to go beyond simple alerting for police and border controls, the interlinking of

⁶ Conclusions of the General Affairs and External relations Council of 14 June 2004

alerts might be put to far wider uses in the name of improving police and judicial cooperation. As a result there is a need for specific safeguards detailing what use can be made of such links and how access is to be limited. Links must be deleted when the corresponding alert is deleted.

5.2 Biometrics

With Eurodac, VIS and now the SIS II there will be a multitude of EU-wide systems incorporating biometric identifiers, operating under differing rules.

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. The Council Conclusions of 14 June 2004 on the functional requirements of the SIS II also defined the criteria to be applied to insert photographs and fingerprints in the SIS II. Both the Decision and the Regulation provide for the inclusion of photographs and fingerprints alongside an alert. In addition, there is a provision allowing such data to be held on individuals for the purpose of dealing with situations where a person's identity has been misused, though such data may only be stored in the system with the 'explicit consent' of the individual in question.

The proposals provide no detail on exactly how fingerprints and photographs are to be incorporated into the system. It is not known, for example, whether biometric identifiers held in the system will be searched using a one-to-many comparison ('identification') or a one-to-one comparison ('verification'). 'Identification' is generally an action taken to recognize someone as being a certain person, whereas the term 'verification' describes an action to confirm that the person being checked is the person on whom an alert was entered.

The JSA has raised this question in previous opinions on the development of SIS II, noting that the reliability of these two systems differs – as do the uses to which they can be put.

The inclusion of biometric data also 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. 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. The Council Conclusions of 14 June 2004 already present a clear indication of the direction that the system might take, with the requirement that photographs and fingerprints should be stored in such a manner as to allow, in the future, functionality for the purposes of identification.

5.3 Regulatory Committee

Various articles refer to the procedure as defined in Article 61 of the Decision – the Regulatory Committee – or to Article 35 of the Regulation regarding the Committee when it concerns the elaboration of detailed rules for the exchange of supplementary information, rules on interlinking and so on. These rules are to be applied by the SIRENE bureaux and are known as the SIRENE Manual. This SIRENE Manual sets out the rules

and procedures governing bilateral or multilateral exchange of supplementary information. This concerns the supplementary information connected to the alert and necessary in relation to the action to be taken. However, there are other subjects to be dealt with by these committees that may have a wider impact. For example, Article 36 dealing with the exchange of personal data that may only have an indirect relation with the alerted object (such as data on a person who bought a stolen object in good faith) leaves it up to the Regulatory Committee to prepare detailed rules for the exchange of these personal data as supplementary information.

Since the SIRENE Manual is closely related to the way data protection principles are implemented in practice, the JSA suggests that the SIS II data protection supervisors should be assigned a formal advisory role in the procedures of the Regulatory Committee and the Committee. This role should be set out in the Decision and the Regulation.

5.4 Proportionality

The principle of proportionality should govern all use of personal data in the SIS II, whether it is a decision on how long to retain data or on whether to disclose data to a third party.

The Schengen Convention includes a useful provision intended to ensure that the principle of proportionality is applied when data are entered in the system: the second sentence of Article 94 (1) of the Schengen Convention reads as follows:

‘The Contracting Party issuing an alert shall determine whether the case is important enough to warrant entry of the alert in the SIS.’

The JSA would recommend that such a provision should be included in the current proposals for the SIS II, so that national authorities will be required to make a decision in each case.

Chapter III

6. The Council Decision

In its assessment the JSA has taken account of the Schengen Convention, the Council Decision of 24 February 2005 concerning the introduction of new functions for the Schengen Information System, the Council Conclusions of 14 June 2004 on the SIS II functions, and the JSA’s earlier opinion on the development of the SIS II.⁷

6.1. General comments

6.1.1 Objective and scope of SIS II

The Explanatory Memorandum to the Decision stresses that the availability of the SIS II as a compensatory measure will contribute to maintaining a high level of security within an area without internal border controls. It will support police and judicial cooperation in criminal matters.

⁷ 19 May 2004 (SCHAC 2504/04)

Convention 108 limits the processing of personal data to specified, explicit and legitimate purposes, and personal data must not be further processed in a way incompatible with those purposes. It is thus necessary to describe the purpose of the SIS II.

The JSA has repeatedly stressed that it should be clear what the SIS II is intended to do and how. Articles 1 and 2 of the Decision combine the very general objective of ‘maintaining a high level of security’ with the role of the SIS II as an instrument for the exchange of specific information for the purposes of controls on persons and objects. These are two different proposals: information exchange for the purpose of controls on persons and objects is specific, while the possibility of information exchange for general police and judicial cooperation is much wider.

In view of the principle of purpose limitation, the opening articles should describe the purpose of the SIS II in clear and explicit terms. Future plans for using the SIS II, creating interoperability with the Visa Information System, and further uses of biometric data (see the Council Conclusions of 14 June 2004) already demonstrate that it is of the utmost importance to have a clear view of the purpose of the SIS II.

The Council should thus make a clear decision on whether the purpose of the SIS II is to be limited to police and judicial cooperation by supporting the controls of persons and objects, or whether the system is also to be developed as a tool to support police and judicial cooperation in a more general way. If the system is to be used to assist police and judicial cooperation in general, this further cooperation should be specifically defined in the Decision. This is essential not only for the assessment of this Decision (and in particular of those articles dealing with access to and use of the data) but also for any new initiatives further expanding the use of the SIS II.

6.1.2. Retention periods of SIS II personal data.

Recital 14 of the draft Council Decision reads as follows:

‘It should be possible to keep in SIS II alerts on persons wanted for arrest and surrender or extradition as well as persons wanted in order to ensure protection or prevent threats and persons wanted for judicial procedure for a maximum of 10 years, given the importance of these alerts for maintaining public security in the Schengen area.’

This appears to be the only explanation given for the Commission’s proposal to extend to ten years the retention period for the alerts referred to. The current retention of such alerts in the SIS is limited to a three-year period (which can be renewed if necessary).

It may be that an extension of the retention period for certain alerts can be justified. Indeed, the JSA is aware that in a number of Schengen States the three-year retention period is routinely renewed, which has resulted in a de facto increase in the standard period of retention for many alerts. Nonetheless, the Commission has yet to make the case for a ten-year retention period. Ten years seems excessive and it is not difficult to think of problems that might arise – for example, it seems absurd that an Article 23 alert entered on a missing minor might be held in the system long after the individual in question has reached the age of majority.

In any case, any increase in retention periods is only acceptable provided that there is an annual review of the need for continued retention. The legislation should require that these reviews be documented, with reasons given for continued retention.

It should also be stressed that the recent discussions leading to the adoption of the Council Decision of 24 February 2005 concerning the introduction of some new functions for the SIS, did not lead to the conclusion that retention periods should be changed. The JSA would be interested to know the reasons for tripling the retention periods since the adoption of the Council Decision of 24 February 2005.

6.1.3 Transfer of personal data to third parties

Article 48 (1) prohibits the transfer of personal data in the SIS II to third countries or international organisations 'except if explicitly provided for in EU law'. Article 48 (2) then states that 'personal data may be transferred to third countries or international organisations in the framework of an EU agreement . . . guaranteeing an adequate level of protection'. The Explanatory Memorandum does not explain why this derogation is necessary, only stating that it will remain an exception to the general rule. The JSA assumes that Article 48 is intended to facilitate the transfer of data to Interpol and authorities responsible for vehicle registration, but it has a wider implication in view of the reference to third countries and the present proposals to connect the SIS II to the Visa Information System.

The first question that arises is: which third parties is Article 48 referring to? Article 3 of the Decision does not give a definition of a third party. The second question concerns the role of the controller. Which bodies will possess the power to make decisions regarding the transfer of data to a third party – and how will this be done?

As it is, this derogation is far too wide. If it is to be possible to transfer data to third parties, 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, among other things, the conditions that must be satisfied before data may be transferred, and whether access will be granted to private organisations as well as public bodies. The principle of proportionality should serve as a guiding principle when making such decisions.

6.1.4 Access by Europol and Eurojust

One of the specific examples for allowing transfer to third parties is the proposed data transfer to Europol and Eurojust. Allowing such organisations access 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.

The proposal is that Europol (and Eurojust) will have 'the right to access data contained in alerts' where such data 'is necessary for the performance of its tasks'. The provisions on access must make it clear that Europol is not entitled to information on individuals wanted for offences that fall outside its competence (this is also the case with Eurojust).

There will be a significant quantity of data held in the SIS II, which Europol and Eurojust should not have access to. For example, Article 15 of the Decision allows alerts for arrest to be entered in the SIS II on the basis of a European arrest warrant, but the range of offences covered by the European arrest warrant extends well beyond those offences for

which Europol is competent. Europol and Eurojust must not have routine access to SIS II data, and there ought to be safeguards in place to ensure that these bodies cannot access information that they are not entitled to see.

On 3 August 2005 the Chairman of the Article 36 Committee requested the JSA to comment on the technical solution created for granting Europol access to SIS. The JSA intends to adopt its position on this subject in October. For further comments on access by Europol and Eurojust, the JSA refers to its comments on Chapter XII (Article 56-58) of the Decision.

6.2. Comments per article

Article 2

See comments under 6.1.1.

Article 4

This article describes the technical architecture and ways of operating the SIS II. The SIS II is composed of a central database, one or two access points and a common infrastructure. The Commission will be responsible for the operational management of the SIS II including the security and confidentiality aspects thereof (Articles 12 and 13 Decision).

Member States will have the possibility to process all SIS alerts in a national copy of the CS-SIS or they may choose to have direct access to the CS-SIS. It is not clear whether Member States may choose both options. This choice might affect compliance with other provisions in the Decision such as the logging of processing, and supervision. When assessing the relevant articles the JSA shall further refer to this problem.

Article 6

It would be useful to have more information on the difference between a national system and a national copy. There ought to be a specific provision defining exactly what is meant by a national system, and explaining how this differs from a national copy. Without this, it is impossible to determine where responsibility for data quality, security and controllability lies. There should also be some way of recording the number of copies made, so that it can be ascertained how many copies have been supplied to consulates, for example.

Article 7

Under Article 108 (1) of the Schengen Convention, one central authority was responsible for the national section of the SIS. Furthermore a SIRENE bureau was set up for the exchange of supplementary information. This created a transparent situation in which it was clear who had responsibility for the national part of the SIS. The Decision changes this structure. According to Article 7 (1), Member States should now designate an office which is to be responsible only for ensuring access by competent authorities. There is no

longer an obligation to designate one authority responsible for the national copy of the SIS. This responsibility seems to be dispersed over those authorities who process their alerts in the national copy and the SIS II. The lack of one central authority with responsibility may create serious problems in maintaining the national copy, data quality, control and supervision. For example, who will be responsible for compliance with the provisions concerning security and confidentiality? The JSA suggests that this provision should be reconsidered.

Article 7 (2) describes the task of the SIRENE authorities. These authorities shall have the task to exchange all supplementary information and to verify the quality of the information entered into the SIS. The JSA understands that this control function will be limited to data processed by the Member State of the SIRENE authorities.

The term ‘quality of the information’ seems to refer to the definition of data quality in Convention 108, which includes principles such as fair and lawful processing, collection and use, adequacy and relevancy and the need to keep data accurate and up to date. Since responsibility for the processing of personal data in the national copy and in the SIS II is left to the different alerting authorities and no other relationship between those authorities and the SIRENE authorities exists than providing the supplementary information, the SIRENE authorities shall not be able to fulfil the task of verifying data quality.

Article 1 (1) of the Council Decision of 24 February 2005, describes the task of the SIRENE authorities. This decision does not mention a task for the SIRENE authorities as now proposed in Article 7 of the Decision. Since no arguments are presented supporting the present proposal to change the task of the SIRENE authorities, the JSA suggests that this provision should be reconsidered.

Article 9

This article deals with the technical compliance of the national systems of the Member States and compatibility with the SIS II, and the national copies of the data of the CS-SIS database.

The philosophy behind the SIS has always been that the national SIS databases should be identical (see Article 92 (2) Schengen Convention). However, Article 9 (2) stipulates that ‘where relevant’ the data in the national copies should be identical and consistent with the CS-SIS. Furthermore, Article 9 (3) repeats this wording, stating that ‘where relevant’ Member States should ensure that a search in such a copy produces the same result as a search performed directly in the CS-SIS. What is the purpose of this provision? When would it be acceptable for data in the national copy to differ from data in the CS-SIS? Does the need to comply with the search results in the CS-SIS also imply that the search possibilities in the national copies should be limited to those in the SIS II, or is a Member State free to choose the accessibility of the SIS II data? Would it be possible, for example, for a Member State to search on biometrics using a one-to-many comparison, even if the SIS II is constructed to allow only a one-to-one comparison? ⁸

In view of the joint character of the system the JSA advocates that national copies should be identical.

⁸ See also the JSA’s previous opinion (SCHAC 2504/04)

Since the SIS II processes personal data of all Member States and, in comparison with the present SIS, considerably more types of data (biometrics and additional information such as the data relating to the European arrest warrant), the JSA is in favour of an obligation on Member States to ensure that the way the data in the national copy may be searched should be identical as in a search in the SIS II. Member States should not be able to search the SIS II using different criteria. Owing to the joint character of the system Member States should not be able to override the legal basis for the SIS II by using the possibility to do so presented by Article 13 (1) of Directive 95/46. The phrase ‘where relevant’ should be deleted. There should be some way in which Member States can check whether databases are identical. The JSA urges the Council to amend this article in that sense.

Article 11

The JSA assumes that the reports that Member States will be required to provide to the Commission will be limited to processing that takes place in the SIS II.

Article 14

The JSA welcomes the requirement to log all processing operations in the SIS II. It is a good contribution to data protection compliance. Article 14 (5) describes data integrity as one of the reasons for the Commission to access these logs. Since the term data integrity also includes the activities for up-dating SIS II data and thus related to the content of the data, the JSA would like to receive more information on the role of the Commission in checking data integrity.

Articles 23 and 24

Article 23 states that the objective of this alert is to place the alerted individual under temporary police protection. However, the access rights to these data as described in Article 24 introduce another objective: communication of the whereabouts of the missing person. The JSA suggests combining all the objectives in Article 23.

Article 27

Article 27 describes the alerts on persons wanted for judicial procedure. It is an almost exact copy of the alert referred to in Article 98 of the Schengen Convention. The only difference is that the purpose of alert in the Schengen Convention aimed at communicating the place of residence or domicile. In the present text the term ‘communicating’ is changed to ‘ascertaining’ which content is more focused on investigative activities.

Article 30, dealing with the execution of the alert only refers to the communication of the place of residence or domicile. In order to prevent any misunderstandings on the action to be taken the JSA suggests to replace the term ‘ascertaining’ in Article 27 with ‘communicating’.

Article 34

See the general remarks under 6.1.2.

Article 36

Article 100(2) of the Schengen Convention allowed personal data to be exchanged relating to an alerted object in accordance with the Schengen Convention. This exchange via the SIRENE bureaux was subject to the provision in Title VI of the Schengen Convention: specific rules on the exchange of personal data and data protection.

The present Article 36 also allows the exchange of those data in accordance with the Decision. However, the Decision does not provide for specific data protection rules on the exchange of supplementary information. It is therefore not clear to which data protection rules the Decision refers. In view of the need for a specific and comprehensive legal instrument, the JSA advocates specifying which rules shall govern the processing of these data.

Article 39

Article 39 contains a list of categories of personal data necessary for the purpose of identifying a person in view of a specific action to be taken. This list differs from the list as adopted by the Council Decision of 24 February 2005. Although some of the new data may contribute to the identification of a person, the JSA is somewhat concerned about this apparent change of views on what is necessary in order to identify an individual. Where the Council Decision of 24 February 2005 relates to objective physical characteristics not subject to change, the present Decision widens this to include characteristics not subject to frequent change. The JSA would like to be informed about the motives for this change and about the kind of data involved.

Article 39 also includes the name of the authority issuing the alert. In view of the purpose of the data as referred to in Article 39: the identification of a person, these data are not necessary for that purpose. The data needed for taking the appropriate action, such as the data referring to the alerting authorities are defined as the additional data (see definition of these data in Article 3). Although no explanation is given, the only reason for adding these data seems to be to enable Europol and Eurojust to contact the alerting authority in case these data are of interest for these authorities. This, however, is not covered by the purpose as defined in Article 39 (2). Data processed for the sole purpose of allowing Europol and Eurojust to take further action cannot be seen as data necessary for the purpose of identifying a person.

The following points should also be addressed. Article 39 (2) refers to the identification of persons. The term 'identification' is also used in Article 44 and in Recital 15 dealing with the use of biometrics. In view of the function of the SIS II, and the way it will be constructed, the definition of this phrase may include a use of data that is not covered by the Decision. As explained above, the term 'identification' is generally used to express an action intended to recognize someone as being a certain person. This definition includes actions that may go beyond the scope of the SIS II. The JSA therefore advocates using the term 'verification'. This phrase expresses exactly what the SIS II as an instrument for the control on persons is intended to do.

Article 39 (3) refers to the technical rules to be established by the Commission for entering and accessing the data referred to in Article 39 (1). The JSA urges the Commission when establishing these rules to use verification as the only reason for accessing data.

Article 40

In relation to Article 40 (1), the JSA refers to its comments in under 5.2 concerning Article 9 of the Decision. The system of searches in the national copies of SIS II should be the same as in the direct access to SIS II.

Article 42

Article 42 (3), allows a Member State to keep in its national file SIS II data in connection with which action has been taken on its territory. It should be clear that this right is limited to the action taken in a particular SIS II alert. A similar right is described in Article 47 (2). The JSA suggests amending Article 42 (3) to bring it into line with the text used in Article 47 (2).

Article 43

Paragraph 4 of this article describes the procedure in case Member States differ in their opinion of whether data in the SIS II are lawfully processed, accurate and up to date. The Schengen Convention introduced an obligation for the Member State that did not issue the alert to submit the case to the Joint Supervisory Authority (Article 106(3) Schengen Convention) in case no agreement between the Member States was reached. The present provision changes this obligation to a voluntary action. In view of the interests at stake for the data subject, the obligation to submit the dispute on data quality to the supervisors should remain. The JSA suggests that this provision should be amended accordingly.

In its report on the inspection on Article 96 Schengen Convention alerts, the JSA recommended that Member States should review their alerts on a regular basis. In view of this, the JSA welcomes the obligation on Member States to review their alerts at least on an annual basis. (See the comments made under 6.1.2.)

Article 46

The JSA refers to its general comments under 5.1.

Article 49

This first article in Chapter X of the Decision dealing with data protection expresses the application of the principles of Convention 108 on the processing of personal data in application of the Decision. As explained above, the applicable data protection principles on the processing of SIS II data are to be found in Convention 108 and Recommendation No.R (87) 15. These principles have to be applied by the Member States party to that Convention and Recommendation. However, the Commission is bound by Regulation 45/2001.

The Decision makes a clear distinction between the responsibilities of the Member States and the Commission taking into account the specific nature of the SIS II. Chapter X of the Decision apparently makes the same distinction linking Member States' responsibility for data quality to the data subject's rights (see Article 51) and the role of the controller (see Article 50). This should be taken into account when specifically defining the role of the controller (see JSA recommendation under 4.2.2 of this opinion).

Article 50

Article 50 would appear to be a combination of two separate rights. The right to information (as set out under the first part of Article 8 of Convention 108 and Articles 10 and 11 of Directive 95/46/EC) and the right of access (as set out under the second part of Article 8 of Convention 108 and Article 12 of Directive 95/46). The right of access is already regulated under Article 51 of the Council Decision, and consists of the right of individuals to establish whether or not there are data processed on them. This right can only be exercised on request.

Article 50 deals, on the other hand, with the right to information, which is intended to guarantee the fair processing of personal data. The duty of the data controller is to provide the individual with information in regard to the existence of certain data processing, namely the conditions under which the individual may exercise the right of access, rectification and deletion. Therefore, there may be derogations from the right to information in specific circumstances; but this right cannot be fulfilled on request.

The JSA would urge the Commission to redraft this provision.

Article 51

This article regulates the procedure to be followed when a data subject wants to invoke his right of access, rectification and erasure. It follows the procedure as described in the Schengen Convention and adds a time period in which the data subject should have received its answer. Although the JSA welcomes such a strict rule, it seems strange that Article 51 sets such a rule and at the same time refers to the national law of a Member State.

Article 51 (4) should include a requirement for the data controller to weigh-up the reasons for and against providing access. Rather than issuing a blanket refusal, the controller would be required to consider each case on its merits. The individual should be guaranteed a reply to any request for access.

Article 51 (5) introduces a time limit in which the data subject must be informed about the follow-up given to the exercise of his right of rectification and erasure. The six months time limit seems to be too long in view of the interests at stake. The JSA suggests a limit of three months.

Article 52

This article is practically the same as Article 111 Schengen Convention. There are, however, three important differences. The wording of this article seems to require that the

data subject seeking a remedy should be in the territory of a Member State. The Schengen Convention did not require this. Any person, whether in a Member State or not, should always have the right to seek remedy. The limitation of the rights of the data subject as suggested by Article 52 is not justified. The JSA therefore urges the Commission to amend the first sentence of Article 52. The first paragraph of Article 111 of the Schengen Convention could be used as an example.

Furthermore, the Schengen Convention stated that such an action could be brought before a court or the authority competent under national law. The Decision only refers to courts. Since the national law in some Member States foresees a procedure before an authority – in most cases the national data protection supervisor – the JSA urges the Commission to amend the text of Article 52 in that sense.

Any action as referred to in Article 52 could involve data entered in the SIS II by another Member State. Since data may only be modified, added to, corrected or erased by the Member State entering the data in the SIS II, Article 52 can only be effective if Member States recognise the decision of a court or competent authority of another Member State. Article 111 (2) of the Schengen Convention introduced this mutual recognition. However, Article 52 does not create a system of mutual recognition, and this might seriously undermine the position of the data subject. The JSA recommends the introduction of a system of mutual recognition similar to the that in Article 111 (2) of the Schengen Convention.

Article 53

According to this article an independent authority of a Member State shall monitor the lawfulness of the processing of personal data in the SIS II. Article 53 limits this monitoring to the processing on the territory of that Member State. This limitation might cause a gap in the monitoring of the processing. Member States have a choice to have either a national copy of the SIS II, which will most likely be on their territory, or to use the SIS II directly instead of a national copy. In the latter case the implication of Article 53 will be that no independent supervision by a national authority will take place on the lawfulness of the processing of the alerts from that Member State. Since the supervisor of the SIS II will not be in a position to monitor the lawfulness of Member States' data, this creates a gap in the system of supervision.

The JSA proposes linking supervision by national supervisors with the responsibilities for data quality as referred to in Article 43 of the Decision. A national supervisor of a Member State entering personal data in the SIS II would then be responsible for monitoring the lawfulness of the processing irrespective of the choice of that Member State to have a national copy or to have direct access to the SIS II.

With regard to Article 53 (3), the JSA refers to its earlier comments under 4.2.3.

Articles 57 and 58

These articles begin with the following text: *'Where the access to the SIS II by Europol/Eurojust reveals the existence of an alert in the SIS II which is of interest for Europol/Eurojust. . .'* This opening line clearly demonstrates a use of the SIS II that has no relation with controls on persons and objects (see 6.1.4). Europol and Eurojust shall most likely use the SIS II alerts as a supplementary source of information. In view of the

functionality of the SIS II, the access of these organisations to the SIS II is limited to searches on persons whose data are already processed by them. Any other possibility for searching should not be possible. The JSA recommends that Articles 57 and 58 be amended accordingly.

This alone would not prevent Europol and Eurojust from accessing personal data that do not fall within their mandates. The JSA therefore suggests that a study be initiated to elaborate which measures can be taken to create a situation guaranteeing that Europol and Eurojust can only access personal data falling within their mandate. One of the solutions might be that the Member States before entering the data in the SIS II may add a specific flag to the data, thus signalling data to be of interest to Europol or Eurojust.

Article 62

The Decision (and the Regulation) are intended to replace Articles 92-119 of the Schengen Convention. However, Article 126 (1) of the Schengen Convention includes a provision allowing Contracting Parties to request the JSA to ‘deliver an opinion on the difficulties of implementing and interpreting this Article’. The Commission should address this apparent oversight.

Chapter IV

7. The Regulation

7.1 General comments

7.1.1 Objective and scope of SIS II

The Explanatory Memorandum to the Regulation stresses that the availability of the SIS II as a compensatory measure contributes to maintaining a high level of security within an area without internal border controls. According to that memorandum, the Regulation rules on the processing of SIS II data supporting the implementation of policies linked to the movement of persons part of the Schengen *acquis*. The Explanatory Memorandum, referring to Article 61 of the Treaty establishing the European Community, also refers to the prevention and the combating of crime.

The heading of the Regulation however only refers to the articles 62(2)(a) and 66 of the Treaty establishing the European Community. Both Directive 95/46 and Regulation 45/2001 limit the processing of personal data to specified, explicit and legitimate purposes, not to be further processed in a way incompatible with those purposes. In view of this, the JSA assumes that the Regulation limits the processing of the SIS II to the purpose of refusing entry to the territory of the Member States by exchanging information for the purpose of controls on persons and objects.

7.1.2 Access to the SIS II

Article 2 (1), dealing with the scope of the SIS II, describes the purpose of the system as the processing of alerts for the purpose of refusing entry into the territory of the Member States. Articles 17 and 18 defining the authorities that have the right to access the system, limit access to those authorities responsible for control of persons at the external borders

and other authorities involved with the execution of immigration laws. The authorities responsible for police and customs checks carried out within the Member States that had access to these data according to the Schengen Convention (Article 101) are now excluded. They are, according to the Regulation, not granted access. The JSA questions whether the Regulation intends to exclude these authorities, or whether the Regulation aims to leave it up to the Member States to use Article 13 of Directive 95/46 to grant access to police and custom authorities.

The JSA reiterates its view as explained under 4.2.1 that the Regulation should be seen as a comprehensive legal instrument. Transparency is best served by a system comprehensively regulating access to the SIS II in the Regulation.

7.1.3 Comparable comments on articles

The JSA refers for its comments on the following articles to its comments on similar articles of the Decision:

Regulation	Decision
Article	Article
6	6
7	7
9	9
14	14
23	42
24	43
25	44
28	50
30	52
31	53
36	62

7.1.4 Comments per article

Article 15

The JSA recently initiated a Schengen-wide study of Article 96 alerts to see whether there were differences in the application of Article 96 (1). Around 90% of alerts in the SIS have been entered under Article 96, on third-country nationals refused entry to the Schengen area.

At the request of the JSA, the national data protection authority in each Schengen State reviewed the national procedure that precedes the decision to enter an alert under Article 96. At the same time, existing Article 96 alerts were examined to ensure that they had been entered in accordance with the relevant legal provisions.

There were significant differences in the number of alerts entered in the various Schengen States. Although these variations are caused by numerous factors, ranging from migratory flows to differences in national legislation, the JSA suggested that the situation might be improved if the reasons for creating an alert were further harmonised throughout the Schengen area.

The Commission appears to have reached the same conclusion: Recital 10 of the draft Regulation explains that it is ‘appropriate to further harmonise the provisions on the grounds for issuing alerts to third country nationals for the purpose of refusing entry’, and goes on to state that ‘The grounds for issuing such alerts, their purposes and the authorities with right to access them should be more homogenous.’ But to what extent are the proposed provisions likely to achieve this objective?

Article 15 (1) would appear to be less open-ended than Article 96, in so far as it makes reference to European legislation featuring the kind of offences for which an alert should be entered in the system. Apart from this, however, it is not clear what changes have been made to harmonise the reasons for entering alerts, and there would still seem to be a lot of discretion given to authorities responsible for deciding when an alert is justified (though there is a proposal for a Directive on common standards and procedures to be followed when returning third-country nationals).⁹

Article 96 (1) of the Schengen Convention stated that alerts were to be entered in the SIS ‘on the basis of a *national alert* resulting from decisions taken by the competent administrative authorities or courts [emphasis added]’; Article 15 of the draft Regulation does not include this requirement for a national alert, which may be no bad thing, as the JSA’s findings suggest that this requirement had been subject to wide interpretation in the different Schengen States, and in some cases there was no evidence that a national alert was ever issued.

Article 20

In its Article 96 inspection, the JSA also found that alerts entered in similar circumstances were being retained for different periods in the different Schengen States. This results in a situation where the length of time an individual features in the system might depend on the country that entered the alert. The JSA recommended that there should be a standard period of retention throughout the Schengen area.

Article 20 (5) of the Regulation introduces a provision whereby alerts will automatically be deleted five years after the decision in Article 15 (1) has been taken, unless the Member State decides that it is necessary, in accordance with Article 15, to retain the alert. This appears to have replaced the requirement in Article 112 (1) of the Schengen Convention to review the retention of personal data in the SIS no longer than three years after they were entered. The JSA would reiterate that personal data must not be kept for longer than necessary. As well as the automatic five year retention period, the JSA would like to see a shorter period of review to ensure that personal data can be deleted if they are no longer needed.

Article 20 describes a situation in which there is an obligation to erase an alert. An alerting Member State should erase an issued alert when it becomes aware that the formal status of the person involved is changed by an action of another Member State. It might improve the quality of the data in the SIS II when a Member State that granted the citizenship or in the situation as referred to in Article 20 (3), after checking the SIS II informs the issuing Member State of the change in the status of the person involved. Article 20 should provide for such an obligation.

⁹ Proposal for a Directive of the European Parliament and of the Council on common standards and procedures in Member States for returning illegally staying third-country nationals COM (2005) 391 final 2005/0167 (COD)

Chapter V

8. General comments on the Regulation regarding the access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates.

The Commission presented its first proposal for such a regulation in August 2003.¹⁰ In that regulation, based on Article 71 of the Treaty of the European Community (Transport), the Commission proposed a new Article 102A of the Schengen Convention allowing authorities responsible for vehicle registration certificates access to certain SIS data. The motivation to grant this access was the need to have access to these data to perform their tasks, more specifically for the administrative purposes of properly issuing vehicle registration certificates.

In the present proposal for the vehicle registration Regulation all the conditions set out in the JSA's opinion of 1 December 2003 are taken on board.¹¹ However, Article 71 is not the correct basis for this Regulation, as the proposal has little, if anything, to do with transport policy.

The need to have a comprehensive legal basis for the SIS II as advocated by the JSA and its call to define specifically the purpose of the SIS II, access by vehicle registration authorities could perhaps be facilitated by an amendment to the Decision in which access for these authorities could be regulated. The JSA suggests that this option be considered further.

The JSA is confident that the Decision and the Regulations will be reviewed in the light of the suggestions and remarks set out in this opinion. The JSA also reaffirms that it is ready to contribute to the ensuing discussion in a constructive manner.

Brussels, 27 September 2005

Ulco van de Pol
Chairman

(Signed in his absence by the Data Protection Secretary)

¹⁰ COM (2003) 510

¹¹ SCHAC 2509/03

ANNEX

Overview JSA Schengen recommendations in respect of the proposed legal basis for the new Schengen Information System

General recommendations

1. The Decision and the Regulation should be viewed as a comprehensive legal instrument for SIS II.
2. Any solution to create a comprehensive legal instrument for SIS II should contain at least some form of vade mecum which could list all the rights that will exist in relation to the SIS II and provide a clear hierarchy of applicable legalisation
3. The Commission and Member States should be designated as joint controllers of the system: with the Commission responsible for its specific tasks as described in the proposals, and each Member State having responsibility for the data it processes in the system. The legal basis should make it clear where the division of responsibility between the Commission and Member States lies.
4. There ought to be provision for an institutionalised joint role for the national data protection authorities and the EDPS in supervising SIS II.
5. It should be specified when links between alerts may be made. Specific safeguards should be in place detailing what use can be made of such links and how access is to be limited. It should be assured that links must be deleted when the corresponding alert is deleted.
6. Biometric data may only be used for verifications purposes.
7. The inclusion of biometric data requires a clear legal framework stipulating in exactly what circumstances and for what purposes searches of biometric data may be carried out
8. The Decision and the Regulation should assign the SIS II supervisors a formal advisory role in the procedures of the Regulatory Committee and the Committee.
9. A provision concerning the application of the proportionality principle should be included in the current proposals for the SIS II.

The Council Decision: general recommendations

10. The Council should make a clear decision whether the purpose of the SIS II is limited to police and judicial cooperation by supporting the controls of persons and objects, or whether the system is also to be developed as a tool to support police and judicial cooperation in a more general way. If so, this further cooperation should be specifically defined in the Decision.
11. The retention periods should remain as defined in the Council Decision of 24 February 2005.

12. Any increase of the retention periods should be well motivated and only acceptable provided there is an annual review of the need of continued retention. The Decision should require that these reviews be documented, with reasons given for continued retention.
13. Clear criteria on the transfer of personal data to third parties ought to be set out in the legislation. The principle of proportionality should serve as a guiding principle when making such decisions.

Council Decision, recommendation per article

Article 2

The purpose of SIS II should be described in clear and explicit terms. See the general recommendation nr. 10.

Article 6

There ought to be a specific provision defining exactly what is meant by a national system, and explaining how this differs from a national copy. There should also be some way of recording the number of copies made, so that it can be ascertained how many copies have been supplied to consulates, for example.

Article 7

A national central authority responsible for the national copy should be introduced. The task of the SIRENE bureau should be brought in line with the Council Decision of 24 February 2005.

Article 9

The national copies should be identical with the SIS II.
There should be a single search facility for the national copies and SIS II.

Article 14

The role of the Commission in checking the integrity of the data should be clarified.

Article 23 and 24

The objectives of these alerts should be combined and defined in Article 23.

Article 27

The term 'ascertaining' in Article 27 should be replaced by the term 'communicating'.

Article 34, see general recommendation nr. 11

Article 36

The Decision should be complemented with specific data protection rules on the processing of supplementary information

Article 39

Data relating to the authority issuing an alert are not necessary in view of the purpose of the processing as referred to in this article.

The term "identification in Paragraph 2 should be replaced by "verification".

Article 40

See second comment on Article 9

Article 42

The text of Paragraph 3 should be brought into line with the text used in Article 47(2).

Article 43

There should be an obligation to submit a dispute on the quality of data to the supervisors involved.

Article 46

See general recommendation nr. 5

Article 50

The right of information should not be restricted to exercise on request.

Article 51

Paragraph 4 should include a requirement for the data controller to weigh-up the reasons for and against providing access. The controller is required to consider each case on its merits. The individual should be guaranteed a reply to any request for access.

Article 51(5) introduces a time limit of six months. The JSA suggests a limit of three months.

Article 52

Article 52 should be brought into line with Article 111 Schengen Convention.

Article 53

The supervision of national supervisors should be linked with the responsibilities of Member States for the quality of the data as referred to in Article 43 of the Decision. A national supervisor of a Member State entering personal data in SIS II would then be responsible for monitoring the lawfulness of the processing irrespective of the choice of that Member State to have a national copy or to have direct access to SIS II.

Article 57 and 58

Europol and Eurojust must not have routine access to SIS II data, and there ought to be safeguards in place to ensure that these bodies cannot access information that they are not entitled to see.

In view of the functionality of the SIS II, the access of these organisations to the SIS II is limited to searches on persons whose data are already processed by them. Any other possibility for searching should not be possible.

It should be explored whether Member States before entering the data in the SIS II may add a specific flag to the data, thus signalling data to be of interest to Europol or Eurojust.

Article 62

The role of the JSA Schengen as referred to in Article 126 (1) Schengen Convention should be reconsidered.

The Regulation: recommendations per article

The JSA refers for its comments on the following articles to its comments on similar articles of the Decision:

Regulation	Decision
Article	Article
6	6
7	7
9	9
14	14
23	42
24	43
25	44
28	50
30	52
31	53
36	62

Article 20

The JSA recommends a shorter period of review to ensure that personal data can be deleted if they are no longer needed.

Article 20 should provide for an obligation for a Member State granting the citizenship or in the situation as referred to in Paragraph 3, after checking the SIS II, informs the issuing Member State of the change in the status of the person involved.

The Regulation regarding the access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates: specific recommendation

Article 71 is not the correct basis for this Regulation, as the proposal has little, if anything, to do with transport policy. Access should be provided by amending the Decision.