Schengen Joint Supervisory Authority
Activity Report – January 2004-December 2005

Foreword

It is my pleasure to present the seventh activity report of the Schengen Joint Supervisory Authority, covering the period January 2004 - December 2005.

During that period, the creation of the second generation of the Schengen Information System - the SIS II - involved major developments, in particular regarding its new legal basis, as well as a great evolution in its nature. Indeed, the SIS will go far beyond a border control instrument to become an extensive investigative tool. The Schengen incidence in the first and third pillar of the European Union, and the wide range of functionalities proposed for the SIS II, requires the reinforcement of data protection guarantees and a coherent application of data protection rules.

Using its 10 years of experience in supervising the Schengen Information System, the JSA has played an important and active role in the discussion on the future of the Schengen Information System, not only through formal opinions, but also by closely following the new architecture of the system and providing guidance whenever was necessary.

In this report, the Schengen Joint Supervisory Authority presents an overview of its activities in the discussion on SIS II and its other activities.

I also would like to leave a special note to the new Member States that have joint us in the JSA, and to underline the close and fruitful cooperation of all within the Joint Supervisory Authority.

Finally, I would like to acknowledge the important role of the JSA chairman during this period, Mr. Ulco van de Pol, to whom we mostly owe the presentation of this report.

Isabel Cerqueira Da Cruz
Chairman

Introduction

The Schengen Convention established the Joint Supervisory Authority (the JSA), an independent body charged with inspecting the central section of the Schengen Information System, examining any difficulties of application or interpretation in the operation of the system, and ensuring that the system complies with the relevant provisions on data protection.

This activity report, the JSA's seventh, provides an overview of the JSA's involvement in the development of the second-generation Schengen Information System (the SIS II). It also includes a report of a Schengen-wide audit of the SIS, which the JSA co-ordinated. It concludes by considering how best to secure effective supervision of the SIS in future.

SIS II

In its last activity report the JSA committed itself to scrutinising the development of the SIS II in order to ensure that the new system complies with the highest standards of data protection.

Opinion on the Development of the SIS II

In May 2004 the JSA adopted an opinion on the development of the SIS II with the aim of influencing the decision-makers responsible for preparing proposals for the new system.[1]

The main argument put forward in this opinion was that a decision ought to be taken on the purpose of the system. Although firm proposals on the purpose and functionalities of the SIS II had originally been scheduled to come out of the Council meeting of June 2003, this had not happened – and by November of that year the European Parliament remarked that, 'the Council remains undecided on concrete questions'.[2]

The absence of clear guidance led to a situation where the Commission had no option but to develop the SIS II to be as flexible as possible. Indeed, the Commission listed 'flexibility' as one of the key requirements of the new system.

The construction of a flexible system without a clear stated purpose brings an increased risk of 'function creep', with the information held in the system being used for purposes other than those for which it was originally intended.

The JSA also argued that with a flexible system it would be more difficult to assess the potential implications of the SIS II, as it was unclear what form the system would ultimately take.
The development of the SIS II was piecemeal and lacked transparency, which made it even more difficult for the JSA and others to assess changes in the system's character.

The opinion concluded that the addition of new functionalities, the inclusion of new types of information, and the trend towards allowing a wider range of bodies access to

[1] SCHAC 2504/04 (24 May 2004)
[2] European Parliament Recommendation to the Council on SIS II (20 November 2003)

the SIS II – when combined with the system's proposed flexibility – made it inevitable that the new system would be very different in character from the SIS; evolving from a hit/no hit system into an investigative tool. The JSA stressed that such a change must be accompanied by corresponding changes to the rules on data protection. As a first step towards establishing what additional safeguards might be needed, the JSA recommended a privacy-impact assessment to determine what impact the SIS II would have on the rights of individuals. Such an assessment could also examine whether proposals for the system were proportionate.

The JSA also made a number of specific recommendations, noting that:

- allowing third parties access to the system made it more likely that information in the system would be put to operational use – by Joint Investigation Teams at Europol, for example.

- if biometric identifiers were to be held in the SIS II there would have to be a clear legal framework stipulating under exactly what circumstances, and for what purposes, searches of biometric data may be carried out.

- access to the system should only be permitted if necessary and proportionate. Access ought to be logged, with regular audits to ensure that the information is only being accessed for a legitimate purpose and by those authorised to have access.

- the interlinking of alerts in the system must not allow users unauthorised access to information.

In response to the JSA's criticism of the lack of transparency in the system's development, there followed an almost immediate improvement in communication between the JSA and those responsible for developing the SIS II. Both the Council and the Commission forwarded all new proposals to the JSA directly.

What is more, steps were taken to ensure that the JSA's contributions were dealt with properly. There were a number of meetings between the JSA's chair and Commission officials, and the Dutch Presidency agreed to table the JSA's opinion at a meeting of the Council's Article 36 Committee.

Opinion on the Proposed Legal Basis for the SIS II

On 31 May 2005 the Commission presented proposals for a legal basis for the SIS II, the main part of which was set out in the following documents:

- a proposal for a Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II) (COM (2005) 230 final)

- 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 final)

The JSA met several times to discuss these proposals in detail, finally adopting an opinion in September 2005.

The Commission had prepared a comprehensive legal basis for the SIS II, and the JSA welcomed the fact that data protection requirements had been given such prominence within the proposals.

Nonetheless, the JSA highlighted four fundamental concerns with the proposals.

The first concern related to the system's purpose. The JSA has stressed repeatedly that the purpose of the SIS II should be clear, and that any change in the system must go hand in hand with corresponding changes in the legal safeguards.

Article 1 (2) of the draft Council Decision states that the 'SIS II shall contribute to maintaining a high level of security', which seems much broader than the purpose of the SIS as defined under Article 93 of the Schengen Convention. The JSA suggested that the opening provisions should provide greater detail on the specific purposes of the system. It is important that there should be a series of well-defined purposes at the outset of the Decision for the sake of clarity – and any proposals to change the system might then be scrutinised in the light of these specified purposes.

The JSA does not object in principle to a change in the purpose for which the system is used, but if the system is to be used for wider policing purposes this must be set out specifically in the legislation, and the implications for the rights of individuals must be taken into consideration.

The second area of concern was to do with establishing which bodies would have responsibility for personal data processed in the SIS II. Determining responsibility for the processing of personal data in the system is important, not least because it will in large part determine the nature of supervision required. The nature of the Commission's role, for example, will have an impact on whether the focus of supervision should be at national or European level.

The JSA is of the view that the Commission and Member States will be joint controllers of the system: the Commission being responsible for its specific tasks as described in the proposals, and each Member State having responsibility for the data it processes in the system. At the moment neither the Decision nor the Regulation make it clear where the division of responsibility between the Commission and Member States lies; this must be addressed.

The third issue of concern to the JSA was that of supervising the SIS II. 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.

As the SIS requires member states to co-operate by sharing data, the JSA was set up with an emphasis on joint responsibility for the personal data processed in the SIS. Specifically, Article 115 of the Schengen Convention charges the JSA with supervising the technical support function of the SIS; examining any difficulties of application or interpretation that might arise during the operation of the SIS; studying any problems that may occur with the exercise of independent supervision by national data protection

authorities; studying any problems that may occur in the exercise of the right of access to the system; and drawing up harmonised proposals for joint solutions to problems.

The current proposals do not provide for all these essential tasks. In fact, the joint tasks currently carried out by the JSA will be replaced by a requirement to hold an annual meeting of national data protection authorities, to be convened by the European Data Protection Supervisor (EDPS).

The JSA believes that the proposed model of supervision currently places too much emphasis on the central processing, which will be minimal. There are compelling arguments for handing responsibility for supervision of the SIS II to the EDPS, but such a move should not reduce the ability of national data protection authorities to co-ordinate their supervisory activities or to discuss common problems as they arise. Supervision of personal data processed in the SIS II will be the responsibility of national data protection authorities, and the provisions on supervision must include all the tasks set out under Article 115 of the Schengen Convention.

Finally, the JSA was anxious that the legal provisions governing the use of the SIS II should be more user-friendly. The legal framework for the SIS II is complicated. Owing to the complexities of the Schengen legal structure various data protection instruments will apply to the processing of personal data in the SIS II; and the application of these various legal instruments, supplemented by specific provisions in the new proposals, is bound to be a cause of considerable confusion. There is also some question about the extent to which exemptions in Directive 95/46 and Regulation 45/2001 will allow those with access to SIS II data to put these data to other uses. While acknowledging the legal reasons for this complex legal structure, the JSA suggested that the 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.

A summary of the main recommendations made in the opinion is attached in an annex to this report.

<u>What Influence has the JSA had on the Development of the SIS II</u>

The JSA welcomed the comprehensive legal basis for the SIS II, particularly the emphasis on data protection requirements.

It was also encouraging that Vice-President Frattini and the chair of the Article 36 Committee both submitted the proposals for the SIS II's legal basis to the JSA at an early stage and requested the JSA's opinion.

Disappointingly, however, neither the Commission nor the Council seem to have examined the question of the system's purpose in any depth. In its note presenting the JSA's first SIS II opinion to the Article 36 Committee, the Dutch Presidency had remarked that: 'While the development of the SIS II is already well on its way, this might be an opportune moment for the Presidency to facilitate the proposed political discussion on the purpose of the SIS in the future.'[3]

[3] Note 11055/04 (5 July 2004)

Despite this, there appears to have been limited discussion of the system's purpose. Consequently, while the purpose of the SIS II remains broad (arguably broader than before), those responsible for the system's development have yet to acknowledge that the system is changing in nature. There has been no assessment of what impact the new system might have on the rights of individuals – there are no plans to carry out a privacy-impact assessment – and so it has not been established whether any additional safeguards are necessary.

Fortunately, those developing the system have continued to involve the JSA in the decision-making process and on 21 October 2005 the UK Presidency gave representatives of the JSA and the EDPS the opportunity to present their respective opinions to the Council's Schengen Acquis working group. Representatives of the Commission, which is also a member of this working group, agreed on the importance of establishing the general purpose of the system. There was also support for the idea that any agreement on data protection rules must involve consultation of data protection authorities.

Ultimately, it remains to be seen to what extent those developing the SIS II will take heed of the JSA's recommendations, but the JSA welcomes the suggestion, made by the Schengen Acquis working group, that the JSA and the EDPS will be invited to provide a formal view on any amendments made to the draft legal basis.

SIS II in the Wider Context of the Third Pillar

The various Europe-wide information systems such as the SIS are increasingly being viewed as a resource in the wider fight against crime and terrorism.

The links between these EU-wide information systems look set to get stronger: the Commission has said that a Communication on enhanced synergies between the SIS II, the Visa Information System and Eurodac is expected in 2006 [4], and there are plans to examine the 'development of links between the SIS II and the Europol information system' in 2007.[5]

The JSA has worked in co-ordination with its sister authorities, the Europol Joint Supervisory Body and the Customs Joint Supervisory Authority, in an attempt to ensure that data protection arrangements keep pace with developments and that all new policy initiatives in the third pillar receive a comprehensive response.

The JSA joined its sister authorities in calling for a new legal instrument to guarantee a higher standard of data protection under the third pillar. Work on this began following an invitation from a House of Lords Select Committee to submit evidence on data protection arrangements in the third pillar, which prompted all the joint supervisory authorities (including the Eurojust Joint Supervisory Body) to adopt a joint opinion on data protection in the third pillar.

This opinion noted that, as they stood, EU proposals would result in the processing of personal data from different sources on an unprecedented scale, often involving the processing of information on those who are not suspected of any crime. It was argued

[4] Communication on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs, COM (2005) 597 24/11/2005
[5] Communication on the Hague Program: 10 priorities for the next 5 years COM (2005) 184 10/5/2005

that Convention 108,[6] which is the only data protection legislation applicable to all third pillar activities, was too general and that a new legal framework for the third pillar should be developed, with a more specific set of data protection rules for police and intelligence authorities.

These recommendations were taken up by the House of Lords Select Committee which stated in its subsequent report that 'enhanced information exchange in the EU, and the trend towards greater profiling of individuals, necessitate the establishment of a common EU framework of data protection for the Third Pillar.'[7]

The joint supervisory authorities went on to contribute to the preparation of a position paper on this subject, which was then adopted by the Conference of European Data Protection Authorities in Krakow in April 2005.

The need for this new third pillar instrument is of direct relevance to the proposals for the SIS II, as the complexities of the Schengen legal structure mean that while Data Protection Directive 95/46 will apply to the processing of personal data under the Regulation, processing that takes place under the Decision will only have to comply with Convention 108.

In December 2004 Vice-President Frattini, Commissioner responsible for Justice, Freedom and Security, addressed a joint meeting of the JSAs. Vice-President Frattini affirmed the importance of completing the 'the harmonisation of the data protection framework under the Third Pillar', and added that the Commission would seek the help of data protection authorities when 'developing a core of guiding principles for the treatment of personal data under the Third Pillar'.

The Commission's work on developing a third pillar instrument on data protection is now under way.

ARTICLE 96

One of the JSA's tasks is to examine any difficulties of application or interpretation that may arise with the operation of the SIS, drawing up harmonised proposals for joint solutions to problems.

Article 96 of the Schengen Convention provides for SIS alerts on third-country nationals refused entry to the Schengen area.

The JSA decided to initiate a Schengen-wide audit of Article 96 alerts because:

- almost 90% of alerts in the SIS were entered under Article 96
- an Article 96 alert has serious consequences for the person concerned, who will usually be prevented from entering the Schengen area
- the number of alerts entered by different Schengen States differs substantially
- there were claims from some quarters that Article 96 alerts were being issued improperly

[6] Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data

[7] *After Madrid: the EU's response to terrorism*, 5th Report, 2004-05, HL Paper 53

The JSA co-ordinated the Schengen-wide audit of Article 96 alerts, with national data protection authorities examining alerts entered by the competent authorities in their respective countries.

The national data protection authority of each Schengen State completed a questionnaire, providing an overview of the various national laws and procedures governing the creation of an Article 96 alert. This overview was to serve as a basis for the audit.

The next step was to develop a methodology for examining Article 96 alerts in order to establish whether there was compliance with the relevant legislation. This was done with the close involvement of a group of technical experts assembled to assist the joint supervisory authorities in such matters.

The first part of this methodology was a means by which national data protection authorities might check the procedures surrounding the creation of an Article 96 alert to ensure that these met data protection requirements.

The second part consisted of guidelines for national data protection authorities to check the content of Article 96 alerts, allowing them to monitor data quality and to establish whether the alert and the file supporting the alert were in accordance with the relevant legislation.

The Schengen Convention stipulates that alerts can only be held in the SIS for a three-year period (though this period can be renewed if necessary). The audit found that in a number of Schengen States the three-year retention period was routinely renewed, resulting in a de facto increase in the standard period of retention for many alerts. The audit also revealed that there were different retention periods in Schengen States, so the length of time for which an alert is retained could depend on which country entered it rather than the reason for which it was entered.

In some Schengen States the decision to enter an alert in the SIS followed automatically from a decision to refuse a person entry to a Schengen State. Such a system, where national alerts are entered in the SIS as a matter of course, is more likely to result in the creation of unwarranted alerts in the SIS.

Three categories of problem were identified in relation to the content of Article 96 alerts. First, the audit found alerts that had not been entered in accordance with national law. Secondly, there were occasional errors when entering the final deletion date of the alert, which could result in an incorrect period of retention, with data often being held for longer than necessary. The third problem was the discovery of alerts on nationals from EU Member States, despite the fact that Article 96 alerts should only be issued on third-country nationals.

The JSA made a number of recommendations, the main ones being that:

- policy makers ought to harmonise the reasons for creating an Article 96 alert throughout the Schengen area
- steps should be taken to remove the disparity in retention periods for Article 96 alerts in the national sections of the SIS

- national authorities responsible for Article 96 alerts should develop formal, written procedures to ensure that Article 96 data are accurate, up to date and lawful.
- Schengen States where responsibility for data quality is shared between more than one authority ought to adopt a joined-up approach in order to ensure that the highest levels of data quality are guaranteed
- measures should be implemented to prevent Article 96 alerts on nationals from EU Member States

Further Investigations at National Level – An Example

The audit co-ordinated by the JSA prompted a number of national data protection authorities to conduct more in-depth national investigations.

One such investigation, carried out by the Danish data protection authority, found that of the 443 Article 96 alerts entered in the SIS by Denmark, 22 alerts concerned individuals that should not have been the subject of an Article 96 alert, either because they were EU citizens or because they had been convicted of offences that did not meet the criteria set out in the relevant national legislation.

The Danish data protection authority declared that the number of errors had been 'unacceptably high'. The National Commissioner of Police, who is the central authority responsible for the Danish section of the SIS, corrected the errors and provided assurances that procedures had been revised to prevent such mistakes from happening again.

Evaluation of Article 96 Audit

All Schengen States participated in this inspection. This joint effort of national data protection authorities, co-ordinated by the JSA was deemed a success and it served to emphasise the importance of co-ordinated supervision of a Europe-wide system that requires each participating state to fulfil its legal obligations.

Ultimately, the inspection did not provide conclusive reasons for the significant differences in the number of alerts entered by different Schengen States. It is worth noting, however, that although the audit revealed some errors in the application of Article 96, the JSA found no evidence of systematic misuse of Article 96 alerts.

Observers in the JSA

The JSA's rules of procedure stipulate that membership of the JSA can only be granted once a country has implemented the Schengen Convention in accordance with Article 140 of the Convention. If the conditions of Article 140 have not been satisfied, the rules of procedure allow the JSA to grant national representatives observer status without the right to vote. The ten new Member States, together with Ireland and the UK, have observer status in the JSA. As Switzerland has signalled that it will accede to the Schengen *acquis*, the JSA agreed in September 2005 to grant observer status to the Swiss Federal Data Protection Commissioner. It was also agreed that representatives of the data protection authorities of Bulgaria and Romania (which are accession countries) would be invited to attend future meetings.

The Future – Safeguarding Rights

The present proposals for the SIS II will result in the abolition of the JSA. The JSA has made it clear that, while it has no objection to this development as such, it is imperative that any new model of supervision ought to provide at least the same level of co-ordination and supervision that has to date been provided by the JSA.

The activities outlined in this report go some way to demonstrating the importance of a system that allows national supervisors to co-ordinate activities and discuss common problems.

The JSA has an important advisory role, examining proposals to change the Schengen Information System and considering what implications these might have for the rights of the individual. Over the years, the JSA's response to proposals to change the SIS have undoubtedly had some impact on the system's development. In the past the Commission has recognised the importance of the JSA's advice:

'The JSA has played a crucial role issuing opinions and recommendations for the proper functioning of the SIS in line with the rules and rights relating to data protection laid down in the Schengen Convention.'[8]

With the removal of the JSA, however, it is not clear how national data protection authorities will provide such comprehensive advice. European data protection authorities have already called for the creation of a forum in which national data protection authorities can discuss the data protection implications of third pillar initiatives. However, such a forum does not yet exist. There must be some means by which national data protection authorities can work together to prepare advice on new initiatives.

The JSA has also enabled national data protection authorities to co-ordinate supervision of the SIS. The SIS consists of national sections with each state responsible for the personal data entered in its section. By co-ordinating supervision of the national sections, the JSA has ensured comprehensive supervision of the system. The Schengen-wide audit of Article 96 alerts, which was initiated by the JSA, provides a good example of how this co-ordination can work in practice.

The JSA also provides a forum in which national data protection authorities can raise problems involving other data protection authorities. For example, two members of the JSA recently brought before the JSA a difficult case involving the institution of a procedure under Article 111 of the Schengen Convention in the hope of finding a solution.

Finally, perhaps one of the most important features of the JSA is that it allows members to discuss matters of interest and to share their experiences openly. This has been particularly important to those countries that are preparing to accede to the Schengen *acquis*, many of whom have no experience of supervising a system of this kind. It is very important that any new system of supervision should find some way to facilitate the exchange of views and encourage best practice at national level.

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

ANNEX

Recommendations in respect of the proposed legal basis for the SIS II

General

The Decision and the Regulation should be viewed as a comprehensive legal instrument for SIS II.

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 legislation

The Commission and Member States should be designated 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.

There ought to be provision for an institutionalised joint role for the national data protection authorities and the EDPS in supervising SIS II.

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.

Biometric data may only be used to verify identity.

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.

A provision concerning the application of the proportionality principle should be included in the current proposals for the SIS II.

The Council Decision

The Council should make a clear decision on 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 the latter is the case, this further cooperation should be specifically defined in the Decision.

The retention periods should remain as set out in the Council Decision of 24 February 2005.

Any increase in the period of retention must be justified and will only be acceptable provided there is an annual review of the need for continued retention. The Decision

should require that these reviews be documented, with reasons given for continued retention.

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.

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 tin Article 126 (1) Schengen Convention should be reconsidered.

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.