



JUSTICE

**Evidence to the
House of Lords EU Sub-Committee F
on the development of the second generation
Schengen Information System (SIS II)**

August 2006

**For further information contact:
Maik Martin, Legal Officer (EU Criminal Justice)
Tel: (020) 7762 6433 Email: mmartin@justice.org.uk**

Introduction

1. JUSTICE is an independent all-party law reform and human rights organisation, which aims to improve British justice through law reform and policy work, publications and training. It is the UK section of the International Commission of Jurists. JUSTICE has been strongly involved in monitoring the development of a European area of freedom, security and justice and seeks to ensure that individual rights are adequately protected in tandem with the development of efficient police and judicial co-operation in criminal matters. We have closely observed the development of the Schengen Information System and have published a report on the System in 2000 (*'The Schengen Information System – A human rights audit'*).
2. We are grateful for the opportunity to submit written evidence on the development of the second generation Schengen Information System (SIS II), which we believe to be a development meriting detailed and comprehensive parliamentary scrutiny.
3. At the outset of our evidence we would like to point the Sub-Committee to the notorious difficulties for non-governmental organisations such as JUSTICE to obtain up-to-date information about the current state of Commission proposals for legal instruments, such as SIS II, under negotiation in the EU Council. These difficulties severely hamper the ability of these organisations to monitor effectively, and comment on, the legislative process under the Third Pillar. There is indeed a need for considerably greater transparency and timely accessibility of documents at Council level in order to achieve an acceptable level of accountability towards European citizens.
4. In the course of our comments, we will confine ourselves to an analysis of the SIS II as envisaged by the EU Council in the current draft Regulation of the European Parliament and of the Council on the establishment, operation and use of the SIS II ('the Regulation'; based on Commission proposal COM(2005) 236 final) and the Council Decision on the operation on the establishment, operation and use of the SIS II ('the Decision'; based on Commission proposal COM(2005) 230 final). We will not comment on the third SIS II instrument, the Regulation giving access to SIS II data by vehicle registration authorities (COM(2005) 237 final).

Key observations

5. JUSTICE is alive to the necessity to re-evaluate the SIS and improve its functioning in light of the need of new EU member states to participate in the system. Where border controls between member states are being abolished there is a clear need to compensate this openness by means of enhanced information exchange allowing for measures to be taken to protect the safety and security of all people living in the EU.
6. We are concerned, however, that the development and introduction of SIS II is not just being used to accommodate a greater number of member states participating in the system and technically improving the one currently in operation, but also to extend its scope and purpose beyond that of merely compensating for the abolition of border controls between member states. In the context of a growing desire of member states to improve information exchange between judicial, law enforcement and asylum and immigration authorities, the introduction of a new generation SIS should not be used to put in place an information exchange mechanism that goes beyond what is needed to compensate for the absence of border controls between member states. The trend towards a comprehensive information exchange architecture in Justice and Home Affairs (JHA) in the EU needs an open, informed and in-depth debate. The overhaul of the SIS is a good opportunity to engage in such a wider discussion; yet, this does not seem to be what the Commission and Council had in mind when embarking on the process of improving the SIS.
7. It is therefore JUSTICE's main concern that the development of SIS II is not limited to improving the day to day technical working of a border control data exchange mechanism but broadens its scope without adequate prior discussion of the consequences of the planned changes.
8. JUSTICE believes that the present Council drafts of the SIS II Decision and even more so the SIS II Regulation
 - may create considerable confusion as to their purpose and scope and thus
 - may not sufficiently respect the principle of strict purpose limitation of personal data.
9. In respect of the grounds for SIS alerts and the general data protection regime in the Council drafts of both the Regulation and the Decision, we recognise that those drafts

indeed contain certain improvements in relation to the SIS I provisions. However, these drafts also still show significant shortcomings and weaknesses. We particularly believe

- that, on account of the current Pillar structure in EU law, the data protection *regime* governing the SIS II is too complex and confusing;
- that the grounds for issuing an alert under the Regulation leading to the refusal of entry into a member state of the affected person remain too vague and that no efforts have been made to harmonise those grounds for an alert;
- that third country nationals enjoying free movement rights will still be subject to Schengen alerts for immigration purposes;
- that data protection rules in the Regulation and Decision with regard to the exchange of supplementary information and national copies of the CS-SIS remain dissatisfactory and unclear;
- that the information and data access rights of data subjects and the remedies against inaccurate information remain insufficient, with too much leeway given to member states to constrain information and data access rights through blanket references to member states' laws throughout the SIS instruments

Interoperability, purpose limitation and data access under the SIS II instruments

10. JUSTICE's main concern with the draft Council instruments providing the legal basis for SIS II is the unclear scope and purpose of the proposed information system.

Interoperability and purpose limitation

11. Under the general data protection principle of strict purpose limitation of the use of personal data, the scope and purpose of a database has a significant bearing on the group of users who may lawfully access a database and process the data held on it. This principle commands that there be a strict *nexus* between the purpose of a data collection and the use that can be made of the data.

12. It is against the backdrop of the general discussion on the so-called interoperability of EU JHA databases that the concept of purpose limitation in the SIS II becomes a dominant issue. The Commission apparently considers interoperability of databases to be primarily a technical concept (see the Communication from the Commission to

the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among databases in the area of Justice and Home Affairs, 24 November 2005, COM(2005) 597 final).

13. We question this narrow understanding of the concept of interoperability. As the European Data Protection Supervisor in his opinion of 10 March 2006 has pointed out, technical interoperability will inevitably raise the issue of the granting of access of persons or agencies to databases to which they would not have been given access under a strict reading of the original purpose of the respective database. Interoperability in this wider sense is thus likely to involve a redefinition and, necessarily, a broadening of the purpose of a data collection. There would be no need to ensure technical interoperability were it not intended that there should also be interoperability in a legal sense of making lawful access to certain data collections beyond the initial purpose for which the data was collected. In this sense, interoperability might not, as such, conflict with the principle of purpose limitation, as the measure laying down the principle of interoperability would have the effect of changing the purpose limiting the use of the data concerned. However, such comprehensive interoperability of JHA databases could have the effect of rendering the principle of purpose limitation practically meaningless in limiting the access to, and use of, personal data in specific databases.

14. We therefore notice with concern the move at EU level towards general database interoperability and the establishment of a system of increased access to JHA databases for law enforcement purposes by security and criminal justice agencies in the broadest possible sense.

15. One example for this trend is the Commission proposal for a Council Decision concerning access for consultation of the VIS by the authorities of member states responsible for internal security and by Europol for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences (24 November 2005, COM(2005) 600 final) and, more generally, the aforementioned Commission Communication on interoperability of JHA databases of the same day. Both envisage the access by member states' internal security agencies to the VIS for the purpose of fighting terrorism and serious crime. The Communication also discusses granting law enforcement agencies access to SIS II and EURODAC for the same purpose. Defining the legal limit for access by law enforcement agencies, the Commission proposes to use the definitions of terrorism and serious offences as laid

down in the Council Framework Decision 2002/475/JHA on combating terrorism and the Europol Convention and its annex respectively. While these proposals are thus limited in their scope to serious threats to public life¹, member states seem to push for more than that, intent on granting access to all three JHA databases for wider law enforcement purposes not limited to the most serious forms of criminality.

Who will get access to SIS II?

16. The SIS II Regulation and Decision exemplify this desire of member states to extend access rights to the SIS II database to authorities beyond those involved in external border control or checks in lieu of intra-Schengen border controls. Arts 17(2) and 37(2) of the current Council drafts for the Regulation and Decision, respectively, provide for access to SIS II data for *'national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation'*. This provision, which was not included in the original Commission proposal, takes SIS II access rights under the Regulation outside the context of border controls and the compensation for the abolition thereof between the Schengen states, and gives certain authorities involved in the national criminal justice systems the rights to access SIS II immigration data (or, under the Decision, to SIS II data relating to alerts for surrender under the EAW scheme etc). Access will not be limited to terrorism offences or other serious forms of criminality.

17. Furthermore, these provisions leave open the question, who these national judicial authorities with SIS II access rights could be, as they are not defined in the Council drafts. As prosecuting authorities take responsibility for the initiation of criminal prosecutions in most member states, it is obvious that they, and not just courts, will qualify as 'judicial authority' within the meaning of arts 17(2) and 37(2). It is far from certain, whether the wording of these provisions would exclude police forces from the circle of those being granted access to SIS II data under the Regulation and Decision. With some imagination, arts 17(2) and 37(2) could be read as including at least certain forms of police forces mandated by prosecuting authorities to carry out investigations for breaches of the criminal law.

¹ Unavailability of these documents does not allow JUSTICE to verify if this test has been retained in the current Council drafts of the VIS access proposal or whether member states are negotiating a lower threshold in line with the current SIS II Council drafts.

18. Obviously, the SIS in respect of alerts on persons and objects for discreet checks - even in its current, first generation version under art 99 CISA – has, by its very nature, a certain investigative function. However, we think the third-country nationals' part of the current SIS I+ does not. Art 101 CISA does not grant law enforcement authorities access to data held on the SIS. The inclusion of (judicial) law enforcement authorities into the circle of those having routine access to SIS II data may therefore be the starting point for a transformation of SIS II (and particularly its First Pillar part) into a veritable investigative tool for general crime detection and investigation purposes. Similarly, the provisions on interlinking of alerts (art 26 Regulations, art 46 Decision), particularly where combined with the law enforcement authorities' access rights envisaged in arts 17(2) and 37(2) of the Council drafts, will further steer SIS II towards becoming a fully fledged general purpose law enforcement database, rather than one limited to the purpose of being a compensatory measure for the abolition of border controls between member states, as envisaged in recital 5 of the current Council draft Regulation.
19. This wider purpose of the SIS II, consonant with the trend towards technical interoperability and provision of more general law enforcement database access rights, may conflict with the principle of purpose limitation in light of the rather narrow scope of legal bases of the SIS II as laid down in arts 2(1) of both the Regulation and Decision. This narrow core purpose of the SIS II - at least its immigration part under the Regulation – is also reflected in art 21(2) of the draft Regulation, where it states that '*[t]he member states may process the data provided for in Article 15 for the purposes of refusing entry or stay in their territories.*' It remains unclear whether this provision indicates a strict purpose limitation for SIS II immigration data (in the sense of '*may ONLY process...*') or whether it does not have any specific meaning in the context of purpose limitation at all. The wide access rights afforded to judicial authorities under art 17(2) of the Regulation would militate in favour of the latter interpretation. Further clarification of the relationship between arts 17(2) and 21(2) of the Regulation is certainly needed.
20. We wholeheartedly endorse the poignant remarks in the opinion of the Schengen Joint Supervisory Authority (JSA) of 27 September 2005. JUSTICE's concerns about the adherence of SIS II to the principle of purpose limitation are exemplified not only by art 17(2) of the draft Regulation, but also more generally by the failure to include in the Council drafts a provision which was originally contained in the Commission

proposals for the said instruments and which reiterated the importance of the purpose limitation principle for processing and accessing the data held on the SIS II. Arts 16(2) of the Regulation and 39(2) of the Decision as originally envisaged by the Commission provided that *'[t]he data referred to in paragraph 1 shall only be used to identify a person for the purposes set out in this Regulation/for the purpose of identifying a person in view of a specific action to be taken in accordance with this Decision.'* We are disappointed to find this provision removed from the current Council drafts.

- 21. The Commission's and Council's desire to achieve technical (and legal) interoperability between EU databases, the discrepancy between the 'general objective' of the SIS II and the 'scope' of the SIS II legal instruments as amply expressed through the widening of access rights especially for immigration data held under the SIS II Regulation, demonstrate the urgent need for a comprehensive discussion at member states' and EU level of the way information exchange in Justice and Home Affairs should be organised and regulated. This inquiry may prove to be a motor for such a discussion.**

The legal framework for the operation of the CS-SIS

22. On the issue of the management of the central SIS II (CS-SIS) by the Commission and, in due course, by the Management Authority envisaged in the SIS II legal instruments, and its legal accountability, JUSTICE embraces the position adopted by the Schengen JSA in its opinion of 27 September 2005. It does not need repetition here.
23. We would like to point out, though, that the legal data protection regime governing the data processing by the Management Authority does not seem to be sufficiently clear (this is a criticism that applies to the data protection regime and the EU pillar structure in general and is elaborated below under marginal note 38). While those aspects of the work governed by the SIS II Regulation will be covered by that instrument as *lex specialis* and the Regulation (EC) 45/2001 of the Parliament and the Council on the protection of individuals with regard to the processing of personal data by Community institutions and bodies as subsidiary *lex generalis*, no such *lex generalis* at EU level exists for the Third Pillar data processing by the CS-SIS II under the SIS II Decision.

24. The original Commission proposal for the Decision, in recital 21, contained a clarification to the effect that data processing by the Commission (or Management Authority) would also be governed by the Regulation EC 45/2001 mentioned above; however, the proposal did not contain a proper provision to that effect. Without entering the debate on the legal effect of a decision recital, we have to state that we do not have knowledge of whether or not this recital has been retained in the current Council draft of the Decision. Even if this were to be the case, the inclusion of an express provision in the body of the Decision, unambiguously declaring the applicability of the said Regulation, would be called for to ensure applicability of that instrument.
25. The prospective Third Pillar Data Protection Framework Decision would not, as such, apply to the Management Authority since this type of legal instrument cannot be addressed to EU bodies; a further, specific Council Decision would thus be needed to extend the scope of the Framework Decision to EU bodies. Currently, art 49 of the draft SIS II Decision declares that personal data shall be protected in accordance with the amended Council of Europe Convention No 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. **While this Convention provides a minimum basis for data protection, we consider it indispensable that a comprehensive subsidiary data protection regime at EU level is in place to govern the work of the CS-SIS II Management Authority.**

Criteria for Schengen alerts under the SIS II Regulation

26. JUSTICE is disappointed that the chance for harmonising the criteria leading to the issuing of a Schengen alert on refusal of entry or stay of third country nationals under art 15 of the current Council draft of the Regulation may be lost.
27. Alerts under art 15 of the Regulation (the former 'art 96 alerts') represent by far the largest number of all alerts on the present SIS. As the 'Report of the Schengen JSA on an inspection of the use of Article 96 alerts in the Schengen Information System' of 20 June 2005 demonstrates, there is an unacceptable divergence of national practices on the issuing of said alerts. In some member states expulsion decisions lead automatically to an SIS alert; in others a separate decision (and thus a separate verification of the necessity of an SIS alert) is needed. Two member states are notorious for issuing alerts for all failed asylum seekers, other member states do not operate such an automatic alert policy. Endorsing the Schengen JSA's

recommendation in its report, **JUSTICE considers it imperative that the criteria for art 15 alerts be harmonised so that a higher degree of uniformity and consistency of art 15 alert decisions across the EU can be achieved.**

28. While art 15(3c) of the current Council draft of the Regulation now provides for a review of the conditions for issuing alerts three years after SIS II becomes operative and allows the Commission to make proposals for a modification of these conditions *'to achieve a higher level of harmonisation'*, the stricter conditions for an alert proposed by the Commission in its original draft have not been adopted by the Council. Consequently, recital 10 of the Regulation as proposed by the Commission, stating that *'it is appropriate to further harmonise the provisions on the grounds for issuing alerts'* and that *'the grounds for issuing such alerts [...] should be more homogenous'*, has been deleted in the Council negotiations.
29. Regrettably, art 15 of the present Council draft of the Regulation does not lay down more specific grounds for issuing an alert than its precursor, art 96 CISA. Moreover, it appears that some criteria for the issuing of an alert have indeed been relaxed in the current Council draft in the sense that the evidentiary threshold for the issuing of an alert on grounds of a perceived threat to public policy or public security seems to have been lowered: while in art 96(2)(b) CISA the threshold was the existence of *'genuine evidence of the intention to commit [...] offences'*, in the current Council draft the test now is the lower one of *'clear indications of an intention to commit such offences'*. The original Commission proposal for the SIS II Regulation did not even contain a criterion along the lines of art 96(2)(b) CISA or art 15(2)(b) of the Council draft at all. **We consider the evidentiary threshold in art 15(2)(b) of the draft Regulation as unnecessarily low and altogether too vague.**
30. Similarly, the alert criterion of a conviction of a third country national under art 15(2)(a) of the Regulation (the former art 96(2)(a) CISA) remains unnecessarily restrictive; a chance to achieve at least a very basic harmonisation of this criterion along the lines of the original Commission proposal is being foregone. The Commission proposal envisaged an alert for a criminal conviction only in cases where the offence was one contained in the list in art 2(2) of the Council Framework Decision 2002/548/JHA on the European Arrest Warrant; furthermore, the penalty following the conviction would have had to be one *'involving deprivation of liberty of at least one year'*. The current Council draft does not follow this suggestion but rather reverts to the formulation contained in art 96(2)(a) CISA, mandating an alert for a

conviction for ‘*an offence carrying a penalty involving deprivation of liberty of at least one year*’. It seems to us that one subtle, yet significant difference between the Commission proposal and the Council draft is the formulation of the one-year-sentence condition: where a third country national is convicted of an offence *carrying* a minimum one year custodial sentence but is then given a *suspended* custodial sentence, it is doubtful whether this sentence would amount to a penalty involving deprivation of liberty within the meaning of the Commission proposal. Conversely, a suspended custodial sentence where the offence *carries* a sentence of at least one year imprisonment would certainly fulfil the condition for an alert under the current Council draft. JUSTICE believes that the presence or stay in the member state of a third country national whose custodial sentence has been suspended by the sentencing judge cannot, as a rule, be considered a threat to public policy or public security. An alert should therefore not be issued in respect of such a person. While we find it difficult to assess, in full detail, the consequences of the difference in the formulation of the test discussed now, we consider the more narrow Commission formulation of art 15(2)(a) of the Regulation to be preferable for reasons of legal certainty.

31. JUSTICE regrets that neither the Commission nor the Council seem to have made any efforts to tackle the issue of the near automatic SIS alerts for failed asylum seekers in two of the member states. We consider it highly desirable that uniform rules as to the treatment of failed asylum seekers as regards SIS alerts be put in place.

32. We acknowledge, however, the potentially beneficial effect of the proportionality clause for the entry of an alert contained in art 14B of the Council draft. It remains to be seen, though, whether national authorities and courts will give meaning to this clause by applying it robustly in the course of the daily operation of the SIS II.

33. The somewhat unclear effect of the individual assessment clause in art 15(1) of the Regulation on the conditions for the issuing of an alert will be addressed in the following paragraphs.

The inclusion of third country nationals enjoying Community free movement rights

34. The current Council draft of the Regulation contains, in art 15A, a rather awkwardly formulated provision, laying down that art 15 alerts concerning third country nationals

enjoying Community free movement rights shall be made in conformity with rules adopted in implementing the Free Movement Directive 2004/38/EC of 29 April 2004. In art 15(1) of the Regulation, it is also decreed that an alert decision '*may only be taken on the basis of an individual assessment*'.

35. JUSTICE welcomes the inclusion in the draft Regulation of these provisions. They should ensure application of art 15(2) of the Regulation in conformity with the free movement restriction provision for third country nationals contained in art 27(2) of the Free Movement Directive. We think, however, more unambiguous guidance as to the treatment of third country nationals enjoying Community freedom of movement could, and indeed should, be provided in the SIS II Regulation itself. This could be done by incorporating into art 15 or 15A of the Regulation a provision mirroring the said art 27(2) of the Free Movement Directive in light of the ECJ's recent judgment in *Commission v Spain* (C-503/03; 31 January 2006, see below marginal note 38).
36. Such clearer guidance might add more weight to the individual assessment clause now contained in art 15(1) of the Regulation. Generally, though, we remain somewhat puzzled as to the precise effect of the individual assessment clause: while art 15(1) exhorts the member states to carry out an individual assessment as to whether the concerned person's presence in the member state poses a threat to public policy or security, art 15(2) provides in effect that such a threat is to be presumed where the conditions of art 15(2)(a) or (b) are fulfilled. We would thus consider the individual assessment clause to act as an emergency brake in cases where contra-indications to the presumption effectively laid down in art 15(2)(a) and (b) are present and would militate against a finding of a person's presence being a security threat.
37. Generally, however, JUSTICE would prefer a complete ban on SIS alerts for third country nationals enjoying Community free movement rights. Such a ban and corresponding duty to erase existing alerts upon the acquisition of free movement rights under EU law could be modelled on art 20 AA of the current Council draft. **We cannot see the need to treat differently EU citizens (for whom an SIS alert cannot be issued) and third country nationals with free movement rights (who will typically be spouses or close family members of an EU citizen) when it comes to SIS alerts. Both categories of persons can be refused entry under art 27(2) of the Free Movement Directive; thus it smacks of an unjustifiable discrimination to allow SIS alerts for one category of free movement rights holders, but not for the other.**

38. With regard to the ECJ's recent seminal judgment in *Commission v Spain* (C-503/03), we consider that it is the new Schengen Borders Code (Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders, coming into effect on 13 October 2006) that will be affected by the Court's decision. While we do not believe that the continued inclusion of third-country nationals with free movement rights on the 'immigration SIS II' is called for, we consider the current draft to be in compliance with the ECJ's ruling in *Commission v Spain*. It was the SIS-specific automatism of a refusal of entry as a consequence of an art 15 alert under art 11(1) in conjunction with art 5(1)(d) of the Schengen Borders Code (the present art 5(d) CISA) that the Court was most critical of in its decision and not the holding of data of this category of persons on the SIS. **While the Schengen Borders Code is not, as such, the subject of the present inquiry, we think it important not only to consider the *conditions* for an SIS II alert under art 15 of the Regulation, but also the *consequences* of such an alert, some of which are laid down by the Borders Code.**

Data protection considerations

A confusing legal regime under the pillar structure

39. What makes an analysis of the data protection regime governing the SIS II a rather complex if not cumbersome exercise is the fact that the SIS II will be governed by a confusing number of legal instruments on data protection. This is due to two reasons: first, the distribution of *lex specialis* data protection provisions between the different SIS II instruments (the Regulations and the Decision) and the subsidiary *leges generales* contained in the EC Data Protection Directive 1995/46/EC governing data processing by the member states, the Regulation (EC) No 2001/145 governing data processing by Community bodies, the Council of Europe Data Protection Convention No 108 of 28 January 1981 and a prospective Third Pillar Data Protection Framework Decision. Secondly, this proliferation of data protection instruments has its cause in the increasingly anachronistic pillar structure of the EU, which the failed constitutional treaty would have ended. Thus, the SIS II Regulations, as First Pillar instruments, are subject to the subsidiary First Pillar data protection directives and regulations, whereas the SIS II Decision, as a Third Pillar instrument, will provisionally be governed by the Council of Europe Data Protection Convention (as envisaged in art

49 of the draft Decision) and, subsequently, by a Third Pillar data protection instrument.

40. JUSTICE believes that this distribution of data protection provisions over numerous instruments may create a risk of uncertainty for everyone involved in the practical application of data protection provisions to data processing in the context of the SIS II. It can also lead to a curious divergence of data protection standards between the different instruments.

41. One example of such a divergence of standards are the provisions in the current Council drafts governing the transfer of data to third countries. While art 48 of the Regulation would not allow to make available or transfer the data processed under the SIS II Decisions (Third Pillar), data processed under the First Pillar SIS II Regulation would be subject to transfer to third countries under the conditions laid down in the EC Data Protection Directive and the Community Data Protection Regulations. These instruments do not contain a blanket ban on transfer of data held on the SIS II to a third state. We cannot see a reason for this difference in treatment.

42. While we would reiterate our urgent call for the adoption and implementation of a robust Third Pillar Data Protection Framework Decision, **we would like to see the creation of a uniform data protection regime for all data processing on the SIS II irrespective of the pillar under which data is being processed.**

Biometric data

43. JUSTICE shares the concern voiced, *inter alia*, by the EDPS and the Schengen JSA, about extensive reliance on biometric data (photographs and fingerprints) on the SIS II as primary identifiers.

44. We therefore notice with approval the inclusion of special rules for biometric data in arts 14 C and 14 AC of the Council drafts of both the Regulation and Decision, especially the rules on special quality checks of biometric data. We hope that these quality check rules will allow a thorough verification of the accuracy of data, bearing in mind the potential use of fingerprints as identifiers for SIS II purposes under arts 14 C(c) and 14 AC(c) of the current Council drafts. We also most warmly welcome the two-year review clause of the use of the biometrics functionality in arts 14 C(d) and

14 AC(d). We expect this review also to cover any practical problems that might have arisen from the use of biometric data in the context of SIS II.

The rules governing supplementary information

45. We regret that the current drafts of the SIS II instruments only inadequately regulate the provision and exchange of so-called supplementary information. According to the definition provided in arts 3(1)(b) of both the draft Regulation and Decision, this is information which is not held on the SIS II and will be made available in a number of situations enumerated in the said provisions.

46. These situations in which additional information may be exchanged are only defined in the most vague and open-ended terms in art 3(1)(b). Pursuant to arts 8 of the draft SIS II instruments, details of the exchange of supplementary information and the nature of such data will be regulated by the SIRENE Manual, as adopted under the comitology procedure provided for in arts 35(3) of the Regulation and 61 of the Decision. No guidance as to the exercise of this rulemaking power is contained in the SIS II instruments themselves. **Supplementary information may comprise highly sensitive personal data, we therefore believe that laying down rules for the exchange of this information should not be left to the member states acting under the comitology procedure, but regulated in greater detail in the main legal instruments providing the basis for SIS II. To regulate only the conversation periods of such supplementary information in the primary instruments (as under arts 27 of the Regulation and 47 of the Decision) has to be regarded as insufficient.**

Data accuracy and quality

47. JUSTICE is disappointed to notice that the provision in art 24(7) of the Commission's original draft Regulation, requiring member states to review data held on the SIS at least annually, has been removed in favour of a simple duty of member states to ensure that data is accurate (arts 24(1) of the Regulation and 43(1) of the Decision). **We believe that strict, harmonised review periods are an essential and indispensable element for a fair operation of a system such as SIS II, as inaccurate data increases the risk of unjustifiable decisions being taken by member states' authorities.**

National copies

48. Issues of data accuracy arise particularly in respect of national copies of the data held on the CS-SIS II. While the central system will ideally contain an accurate set of data, updated, when necessary, by the relevant member state, use of national copies may increase the risk of relying on, and operating with, outdated and thus inaccurate data. We therefore regret the deletion from the original Commission draft of the SIS II instruments the duty of member states to ensure that the national copies are at all times identical and consistent with the CS-SIS (arts 9(2) of both the Regulation and Decision). The new arts 9(2) only speak of equivalent results which searches in the national copy and the CS-SIS have to yield.

Interlinking of alerts

49. We appreciate the fact that links between alerts as provided for in arts 26 of the draft Regulation and 46 of the draft Decision must not have the effect of widening law access rights and may only occur where there is a clear operational need. However, **we are not convinced that an interlinking of alerts, being essentially an investigative tool, will sit easily with the principle of purpose limitation of the data held on the SIS II.** On the (contested) assumption that SIS II - certainly its immigration part under the Regulation - should not have the function of a tool for general crime investigation purposes, it is difficult to justify the creation of links between SIS immigration data under the Regulation and those of a more law enforcement oriented type under the SIS II Decision. The need to link alerts should thus be very carefully examined.

Data transfer to third countries

50. **While there may be situations calling for a transfer of personal data held on the SIS II to third countries, JUSTICE is surprised at the differential treatment in this respect of immigration data (which will be subject to the third country data transfer provisions of the EC Data Protection Directive) and other SIS data, for which the draft Decision contains a bar on transfer to third countries (art 48).** We would urge the Sub-Committee for an explanation for this difference in treatment.

Rights of the data subject

51. Adequate information and access rights and meaningful legal remedies are a crucial element of an information system, under which alerts can have automatic and harsh consequences, such as the refusal of entry into an EU member state of third country nationals under the Schengen Borders Code.
52. We generally welcome the level of rights accorded the data subject in the current Council drafts of the SIS II instruments. However, we believe that the rights and remedies provided for in the current drafts could be improved, making them more effective for the data subject. In particular, **we are of the view, that the role of member states' national law in determining the extent, exceptions and implementation of those rights and remedies is a too wide-ranging one. A higher degree of approximation or even harmonisation of these safeguards for a fair functioning of the Schengen system is called for.**

Right of information

53. While a right of information of the data subject about the data being held on him or her by the data controller exists for third country nationals under art 29 of the draft Regulation in conjunction with arts 10 and 11 of the EC Data Protection Directive, no such right of information is provided for in the draft SIS II Decision for Third Pillar data. While it has to be acknowledged that the latter category of data may be of a more sensitive nature than immigration data held on the SIS, a right of information with a general national security/safety exception (as in art 29 of the draft Regulation) could and should be provided for without compromising the sensitive nature of the data where this would be an issue.
54. With regard to the exceptions to the right of information of third country nationals contained in art 29(a)-(c) of the SIS II Regulation, we are concerned about the blanket nature of the reference to national law under art 29(c). While the provision lists examples of circumstances in which member states' laws could restrict the information right, this list is only indicative ('... *in particular in order to safeguard national security, defence, public security*' etc). Thus this provision leaves member states free rein to limit the right of information as they please with no meaningful judicial oversight by the ECJ. Restrictive national legislation may even lead to the risk that this important right will be little more than an empty shell in practice.

55. The Commission proposal, however, did not contain such a reference to national laws. **We would urge the Sub-Committee generally to take a strong line on the extent to which the current SIS II Council drafts rely on member states' domestic laws when fleshing out (or rather limiting) the data protection standards and the rights a data subject has to enjoy throughout the EU.** Bearing in mind the differences in domestic data protection standards between EU member states in the area covered by the Third Pillar, the establishment of meaningful and robust data protection standards across the EU depends on the level of harmonisation (or at least significant approximation) of member states' laws in this area. Such harmonisation cannot be achieved by blanket references to member states' laws where limitations of the rights of the data subject are concerned.

56. We also consider the data subject's right of information not to be strong enough. As we have already highlighted in our publication on SIS I in 1999, not only should a data subject be furnished with information that data on him or her is held on the SIS II (and perhaps even what kind of data are stored), but also he or she should be provided with standard information about his or her legal remedies. Art 28(e) of the current SIS II draft Regulation does not go that far. **We believe that legal remedies, such as those provided for in arts 30 of the draft Regulation and 52 of the draft Decision, are only effective where they are practically accessible, in particular, where the individual entitled to the remedy is made aware of its existence and the procedure for claiming it correctly.** It would be desirable to devise a standard 'letter of rights' for data subjects, which would explain the legal remedies available to them in a language they can understand.

Right of access, correction and deletion of data

57. JUSTICE is concerned that the formulation of the provisions governing the data subject's right of access to the personal data held on the SIS II (arts 28 of the Regulation and 50 of the Decision), once again, leaves too much leeway for national laws to undermine the general right of access enshrined in these provisions. It remains unclear how far the substantive right of access under art 28 and 50 of the SIS II instruments reaches and to what extent member states may lawfully make inroads into this general entitlement when regulating the way in which the right of access to the SIS data may be exercised. Harmonisation of domestic data protection standards at a high level can hardly be achieved where there is only insufficient

guidance as to the implementation and enforcement of the abstract right of access to one's personal data.

58. Similarly, the exception to the general rule on access to data contained in arts 28(2) and 50(s) of the current Council drafts attracts concern: according to these provisions, which did not form part of the original Commission proposals, '*communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedom of others.*' The first alternative of the test for the lawfulness of a member state's denial of access to information held on the SIS II appears overly broad and deviates in this aspect significantly from the model provided for in art 13 of the EC Data Protection Directive: according to arts 28(2) and 50(2) access to data may be refused where this would be indispensable for the performance of *any* lawful task of member states' law enforcement agencies.
59. The provisions do not distinguish between lawful tasks of law enforcement agencies of different importance and thus do not contain a balancing requirement obliging member states to weigh the infringement of the data subject's right of access to the SIS data against the likely effects of access to data on the criminal justice system and crime detection and investigation. **Denial of access to the SIS data cannot be considered proportionate in cases where the police or public prosecutors are performing a lawful, albeit quite insignificant, task and where only a denial of access to the SIS II data would ensure that that task was fulfilled. Without engaging in a balancing exercise and robustly applying the proportionality test, denial of access to a data subject's SIS data may amount to a violation of the concerned individual's right under art 8 ECHR.**

MAIK MARTIN

August 2006