Permanente commissie
van deskundigen in
internationaal vreemdelingen-,
vluchtelingen- en strafrecht

Secretariaat
postbus 201, 3500 AE Utrecht/Nederland
telefoon 31 (30) 297 42 14/43 28
telefax 31 (30) 296 00 50
e-mail cie.meijers@forum.nl
http://www.commissie-meijers.nl

[redacted] [redacted]

To Michael Collon
Clerk of Sub-Committee F
Select Committee on the European Union
Committee Office,
House of Lords
London SW1A 0PW

Reference CM06-10

Regarding Comments of the Standing Committee of experts in international immigration, refugee and criminal law on the development of the second generation Schengen Information System (SIS II)

Date 10 July 2006

Dear Member of the Select Committee,

Please find enclosed some general comments of the Standing Committee on the development of the second generation Schengen Information System or SIS II. In these comments we will focus on the draft Regulation on SIS II, based on the revised text as agreed upon during the meeting of the EU Ministers of Justice and Home Affairs of 2 June 2006. We enclose our earlier comments on the draft proposal for a Regulation concerning the Visa Information System as we think the subject of SIS II is closely related to the development of VIS.

We hope you will find these comments useful for your inquiry. Should any question arise, please do not hesitate to contact us.

Yours sincerely,

On behalf of the Standing Committee,

Prof. C. A. Groenendijk
Chairman

Permanente commissie van deskundigen
in internationaal vreemdelingen-,
vluchtelingen- en strafrecht

Comments of the Standing Committee of experts in international immigration, refugee and criminal law on the development of the second generation Schengen Information System (SIS II)

CM06-10

1 Introduction

On behalf of the Standing Committee, we would like to submit some general comments on the development of the second generation Schengen Information System or SIS II. In these comments we will focus on the draft Regulation on SIS II, based on the revised text as agreed upon during the meeting of the EU Ministers of Justice and Home Affairs of 2 June 2006.[1] It should however be underlined that the adoption of this Regulation is to be considered in close connection with other developments in the EU. Firstly, the future use and impact of SIS II will be determined by the final texts of the Decision on SIS II for policing purposes (COM (2005) 230) and the Regulation giving access to SIS II by vehicle registration authorities (COM (2005) 237). Secondly, which authorities will have access to SIS II and the further use of this information will depend on the final decision-making with regard to the proposed Visa Information System (VIS), the future use of Eurodac, and the inclusion of biometrics in the EU databases and the EU passport. The fact that different drafts of these proposals are still circulating, makes it difficult if not impossible to assess the full implications of the future developments at this moment. Thirdly, it is important to be aware that national developments are decisive for the future use of SIS II. Important factors are of course the national criteria on the basis of which data are entered into SIS II and the accuracy and reliability of these data. But it should also be taken into account that the introduction of new technologies for surveillance purposes at the national level, including biometrical identifiers, facial recognition systems, or automated license plate readers for vehicles, could extend the use and availability of SIS II information beyond its anticipated goals.

In the following paragraphs we will deal with the following aspects of the draft Regulation on SIS II:

- Decision-making process
- Operational management – accountability
- Inclusion of biometrics
- Clarity of rules governing collection of and access to data
    a. Criteria of third country nationals to be stored into SIS II
    b. Authorities receiving access to SIS II
- Adequacy of data protection rules – rights of individuals
    a. Applicable rules
    b. Purpose Limitation
    c. Individual rights and legal remedies

2 Decision-making process

The Standing Committee is concerned about the lack of transparency with which the proposals on SIS II are actually adopted. The Standing Committee emphasises that the development of SIS II is an extremely important subject which includes the set up of a very large database, involving the registration of millions of individuals, including family member of EU citizens. This database will have a large impact on the movement of individuals, not only because of the proposed use of biometrics, but also because of the implementation of the principle of interoperability, as proposed by the European Commission (COM (2005) 597). Although the Commission has not yet submitted more specific proposals, the principle of interoperability refers to the common use of large scale IT systems (SIS II, Eurodac, VIS), but also to the possibility of accessing and exchanging data or even merging the different databases. The establishment of SIS II and its shared use with other EU databases require careful scrutiny by the European Parliament and national parliaments. Their involvement has been made difficult by the piecemeal approach with regard to decision-making on SIS II and the other databases. Between 2001 and 2006, different legislative measures, including decisions on the technical features of SIS, have been adopted by the Council. These decisions gradually allowed for an extended use of SIS. Further it should be noted that the original proposals of the Commission differ from the most recent drafts and that these latter texts have been made accessible neither to the general public nor to the national parliaments.

The co-decisive role of the European Parliament with regard to the draft Regulation on SIS II has to be welcomed, as well as the improvements of the final text as proposed by the European Parliament. However, the confidential negotiations between European Parliament, Council, and the European Commission, do not provide any insight why on and on whose behalf final decisions or compromises have been reached. It is still unclear whether the text

[1] For our comments we have used the text as adopted on 6 June 2006, doc. 5709/6/06, see the website of Statewatch: www.statewatch.org.

which has been agreed upon by the EU Ministers of Justice and Home Affairs in their meeting of 2 June 2006, must be considered as the final compromise text between European Parliament, Council, and Commission, or whether this text will receive full scrutiny by the European Parliament, when dealing with it during its plenary sessions. In this regard, the Standing Committee refers to the adoption of the Regulation on the Community Borders Code in 2005.[2] Based on the concerns of the Council and the European Parliament to have this legislative proposal adopted during the first reading of the applicable the co-decision procedure, the compromise text as agreed upon during the tripartite negotiations was considered as the final version even before the public plenary session of the European Parliament. According to the Standing Committee, this chosen procedure of decision-making hampers the transparency of legislative procedures within the EU.

3 Operational management – accountability

In a note of 15 May 2006 on the issue of long-term management of SIS II, the Austrian Presidency proposed to set up a special Agency for the management of SIS II, and possibly also for Eurodac and VIS.[3] In the text of the draft Regulation on SIS II as agreed upon on 6 June 2006, this proposal has been included in a new Article 12 dealing with the tasks and responsibilities of a "Management Authority". This Management Authority should after a transitional period perform the tasks of the Commission with regard to the supervision, security, and coordination of relations between Member States and the provider of SIS II. The Standing Committee is in general concerned about the institutional consequences of the set up of new agencies in the legal framework of the EU. The set up of a separate agency or Management Authority might have its practical and budgetary benefits, but it should be prevented that such authorities receive EU responsibilities and competences and at the same time will be able to operate quite autonomously from the EU institutions. According to the Standing Committee, the set up and the functioning of such agencies, including the Management Authority, should be made dependent of the following guarantees:

- full competence of the European Court of Justice to assess the lawfulness of the activities and decisions of these agencies or authorities;
- clear rules on their liability;
- clear and coherent rules with regard to the responsibility of the European Commission, and;
- application of the general EU rules on access to documents of the EU institutions.

4 Inclusion of biometrics

Article 14 C of the draft Regulation as agreed upon in June 2006, includes the option that biometrical data to be entered into SIS II will be used as identifier. Or with other words, SIS II will be searchable on the sole basis of biometrical data such as photographs or fingerprints without needing additional data on the person concerned such as name and surname. This use of biometrics as identifier has been explicitly rejected by the European Commission, but also by the European Data Protection Supervisor and the Article 29 Working Group, on the basis of the fact that the technological reliability does not allow for a secure and reliable identification. Using biometrics as sole identification key still entails a too high risk of false identification or false non-identification (compare: 'false rejection rate' and 'false acceptation rate'). Even if only one or a half percent of the persons would be wrongly identified on the basis of biometrical data in SIS II or VIS, considering the millions of person to be recorded in these databases, still the number of persons affected by automatic negative decisions will be much too high. Different organisations warned for the fact that the use and central storage of biometrics will extend the risk of unauthorised access to these databases, the misuse or manipulation of biometrical data by criminal organisations, and the possible increase of identity theft. These negative aspects, as well as the impact of the use of biometrics for the privacy and human rights of individuals, have not been appropriately taken into account in the decision-making process.

5 Clarity of rules governing collection of and access to data

a. Criteria for third country nationals to be stored into SIS II

The adoption of the Regulation on SIS II would have been an excellent chance to harmonise the applicable criteria for the registration of third country nationals to be refused entry. The original proposal of the European Commission of May 2005 included a useful proposal for such harmonisation. It is regrettable that Article 15 of the draft as agreed upon by the Council in June 2006 returns more or less to the same criteria as included in the actual provision of Article 96 of the Schengen Convention (SC). The actual use of Schengen Information System (SIS) has shown that the implementation of these criteria varies considerably between the Member States using SIS. The difficulties which arise from such differences in interpretation can be illustrated by the annual reports of national data protection authorities and judgments of national courts dealing with decisions based on foreign SIS

[2] Regulation 562/2006 of 15 March 2006, *OJ* L 105/1, 13.4.2006.
[3] Council doc. 9169/06

alerts. It is to be feared that the extended use of SIS II from 15 European states to more then 25 states, will only increase the problems caused by the different interpretations of the criteria as provided in Article 15.

The criteria in Article 15 (2) of the draft Regulation of June 2006, include two important extensions of the applicable criteria compared to the original text of Article 96 SC. Firstly, Article 96 (2) (b) SC requires that a decision to report a person into SIS should be based on 'serious grounds for believing that he has committed serious criminal offences… or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a contracting party.' Based on the proposed Article 15 (2) (b), 'clear indications of an intention to commit such offences' are considered sufficient for registration into SIS II.
Secondly, the proposed Article 15 AA provides that third country nationals may be registered into SIS II on the basis of a decision taken in accordance with Article 15 of the EU Treaty. This new category refers to persons enlisted in the EU terrorist lists based on the travel ban as issued by the Security Council of the United Nations. The Standing Committee is in general concerned about the secret and unclear criteria on the basis of which third country nationals are enlisted as 'terrorists'. The automatic inclusion of these persons into SIS on the basis of which they will be refused entry should be accompanied by minimum guarantees preventing erroneous registration in SIS II. The concerns of the Standing Committee are strengthened by the fact that Article 15 AA (2) includes an exception to the general rule of Article 14D, that an alert cannot be entered without the information on the name, sex, a reference to the decision giving rise to the alert, and the action to be taken. It is unclear how persons enlisted in the EU or UN terrorist list can be registered in SIS II without their names or referring to the action to be taken, unless it is the intention of Member States to enter these persons into SIS II solely on the basis of the use of their biometrical data such as fingerprints.

It is to be welcomed that, as proposed by the Commission, the final text of the Regulation includes the obligation for Member States to erase alerts on persons as soon as the Member State which issued the alert becomes aware that the person acquired EU citizenship (Article 20 AA). The Standing Committee regrets however that the final text does not include the obligation, as proposed by the Commission, to erase data on third country nationals who become family of EU citizens as well. This omission seems to be in contradiction with the judgment of 31 January 2006 of the ECJ in the case Commission v. Spain (C-503/03). In this judgment, the ECJ ruled that the listing of third country national family members of EU citizens in SIS, and more specifically the automatic decision-making on the basis of this listing, infringes the rights of these persons under EC law.

b. Authorities receiving access to SIS II

In the original proposal of the Commission of May 2005, information on third country nationals stored into SIS would only be accessible for authorities responsible for border controls and for authorities issuing visas. Article 17 of the draft Regulation of 6 June 2006 provides that access to information stored into SIS II in accordance with Article 15 will be reserved exclusively to authorities responsible for border control and for 'other police and customs checks carried out within the country, and the coordination of such checks by designated authorities'. Although the Standing Commission welcomes the addition of the words 'exclusively' and 'designated authorities', it should be noted that 'authorities responsible for police checks within the country' still includes an extremely wide category of officials. This implies the use of SIS II and the information on third country nationals therein for other purposes than only border control or visa applications. Although Article 17 A of the Regulation on SIS II provides that users 'may only search data which they require for the performance of their task', it is questionable whether the general provision will prevent police officers to start general searches in SIS II when checking persons within the national territory for public order reasons.

Article 34 (2a) of the Regulation on SIS II includes the obligation for the Management Authority to publish each year statistics showing the number of records per category of alert, the number of hits per category of alert and how many times the SIS II was accessed. It might have been useful if these statistics would also include other information, for example on the authorities which actually obtained access to SIS II, the nationalities of persons stored into SIS II, or on the decisions or measures which have been taken on the basis of SIS II information. This would make it possible to assess the added value of SIS II more completely.

6 Adequacy of data protection rules – rights of individuals

a. **Applicable rules**

The data protection regime applicable to SIS II and other EU databases is complicated by the two pillar dichotomy which accompanies the current legislation. On the one hand, data processing through SIS II falls within the scope of the Data Protection Convention of 1981 of the Council of Europe and, if adopted, the EU framework decision on third pillar data protection. On the other hand, the processing of data on third country nationals to be refused entry as provided in the Regulation on SIS II falls within the scope of the EC Directive 95/46. This latter Directive will also

apply to the proposed VIS, except for the proposed dissemination of VIS data to internal security authorities and to Europol (COM (2005) 600): this would fall under the third pillar data protection rules.

In view of transparency and equality, the simultaneous application of different set of rules with regard to the processing of the same personal information is undesirable. Not only individuals, but also the authorities using these systems need to know which rules apply. The ratification of the Constitutional Treaty of the EU by all Member States would have solved this problem partly because of the proposed collapsing of the three pillars, which could have been an extra motive to extend the application of the EC Directive 95/46 to the general field of EU law. As long as the three pillar construction applies, other solutions will have to be found to solve the problem of divergent data protection rules. One solution could be to adopt on a very short term the proposal for a framework decision on data protection in the third pillar.[4] However, this option should be made dependent on the following requirements.

- Inclusion of a high level of data protection standards in this framework decision.
- The frame work decision should be applied as specification and not limitation of the general data protection principles as included in the EC Directive 95/46 and Article 9 of the EU Charter of Fundamental Rights. This has been explicitly underlined by the Commission in her explanatory memorandum to the proposal of the framework decision.
- The scope of the framework decision should be extended to the use of personal data by Europol and Eurojust and other authorities or agencies using personal information for law enforcement, judicial, or internal security purposes. Aside from the transmission of data between member states, the framework decision should also cover data processing within the member states. It should be prevented that data processing falling within the scope of EU law, would fall outside the scope of EU rules of data protection and, thus, may fall outside the scope of any rule of data protection.
- The individual rights to information and to access, correction, and deletion of data, as well as the right to legal remedies should be in conformity with the applicable rules in the other instruments of data protection. It would be unacceptable if the level of data protection for an individual with regard to the same information in the same database, would be made dependent on the authority having access to this data or the purpose for which this has been transmitted to other authorities.

b. Purpose Limitation

The purpose limitation principle is one of the key principles of data protection. It safeguards the transparency and legality of the use of personal data. The Standing Committee is most concerned about the fact that this fundamental principle is rendered meaningless by actual developments. These developments include in the first place the vague and open definitions of the goals for which new EU data bases are set up. For example, the purpose of SIS is described in the SIS II Regulation proposal as: 'to maintain public policy and a high level of public security, including national security in the territories of the Member States and to apply the provisions of Title IV of the Treaty establishing the European Community relating to the movement of persons in their territories, using information communicated via this system'. The goal of VIS has been presented from the beginning as a 'multifunctional tool'. VIS will not only be used for the implementation of EU visa policy, but also for the fight against illegal immigration and terrorism, and to return illegal immigrants. As we have seen above, a draft has been prepared to give national internal security authorities and Europol access to VIS as well. Secondly, recent proposals of the Commission on interoperability of databases (COM (2005) 597) and the principle of availability (COM (2005) 490) are in absolute contradiction with the principle of purpose limitation. National and European data protection authorities repeatedly underlined the importance of purpose limitation and have warned for the risk of 'function creep'. Allowing the use of personal information, including biometrics, by different authorities for different purposes not only entails the risk of wide dissemination of unreliable information, but will also threaten to infringe the rights of individuals concerned.

c. Individual rights and legal remedies

The refusal of entry based on SIS II, the wrongful identification based on biometrics stored in SIS II or VIS, or the unlawful transmission of personal data to third parties or third countries, all include the risk to violate fundamental rights as recognized in the European Convention in Human Rights and the EU Charter on Fundamental Rights. Both the European Court of Justice as the European Court on Human Rights repeatedly underlined the importance of the right to privacy and data protection, formulating stringent criteria for measures interfering with these rights.[5] At the national level, the German Constitutional Court recently ruled that large scale data searching

[4] COM (2005) 475.
[5] ECJ: C-101/01 *Lindqvist OJ* C7/1, 10.01.2004 and C-456/00 *Österreichischer Rundfunk* in *OJ* C171/3, 19.07.03; ECtHR: *Rotaru*, 4 May 2000, appl.no. 28341/95.

('Rasterfahndung'), a measure which has been used by the police in Germany to trace terrorists by gathering information from different databases, constituted a disproportional infringement of the individual's right to privacy.[6]
Refusals of entry based on SIS information further risk to violate the Community law rights of third-country nationals to enter and reside in a Member State, granted by Directive 2003/86/EC on the right to family reunification or Directive 2003/109/EC on the states of long-term resident third-country nationals. In its judgment of 27 June 2006 in the case EP v Council (C-540/03) the Court affirmed that the first Directive grants a subjective right to family reunification to spouses and minor children without a margin of appreciation being left to Member States (paragraph 60 of the judgment).

Considering the developments described above, the legal protection of individuals is an absolute requirement. Individuals should have the right to accessible and effective remedies with regard to the use of SIS II. The actual practice of SIS shows that a huge problem for individuals is the fact that they often do not know that they are recorded into SIS for the purpose of refusal of entry. They will only discover this when applying for a visa or when being checked at the borders. The Standing Committee regrets that the original proposal of the European Commission to oblige national authorities to inform a person in advance on the processing of his or her data in SIS II (including identity of controller, purposes, potential recipients) has been deleted. The actual new draft only includes the (general) right of the individual to apply for access, rectification, or correction.

Important is the removal of the territorial limitation, as included in the original Commission proposal, with regard to the access to legal remedies. Article 30 (1) of the draft of 6 June 2006 now provides that any person may bring an action before the courts or the authority 'in particular to correct, delete or obtain information or to obtain compensation in connection with an alert involving them'. This means that, different from the original proposal, access to remedies is no longer dependent on whether the person actually is within the territory one of the EU Member States. Especially where it concerns the use of SIS II for the refusal of entry or a visa, it would have been unacceptable if a third country national would not be able to remedy the wrongful use or registration of his or her personal information if he or she would be outside the EU territory. The Standing Committee recommends that this territorial limitation will also be lifted in the other proposals on SIS II or VIS.
Further, the text of the Regulation on SIS II re-introduces in Article 30 (2) the obligation for national authorities to enforce mutually the final national decisions of courts or authorities as meant in Article 30 (1). This provision which already has been included in Article 111 (2) SC, is a very important safeguard for individuals. This provision ensures that decisions taken by independent authorities on the lawfulness of a national alert in SIS will have to be enforced in other Member States as well. The actual practice of SIS shows however that national authorities often are reluctant to enforce the decisions of foreign courts or data protection authorities. The re-inclusion in the Regulation on SIS II could be a new impetus to enforce this mutual recognition. Another problem is caused by the fact that national courts do not always find themselves competent to assess the lawfulness of a foreign decision when dealing with a third country national whose entry or visa has been refused on the basis of a SIS alert. This problem is also due to the lack of harmonised criteria for entering persons into SIS II. One of the solutions to solve this problem could be to extend the competence of national courts to forward preliminary proceedings to the ECJ. This could enable the Court to clarify the applicable criteria and to assess the necessity and proportionality of the measures involved.

Finally, in Article 30 (3) of the Regulation on SIS II, it is provided that the Commission will evaluate the rules on remedies a provided in this Article, two years after the Regulation enters into force. This evaluation will be an important tool to assess both the accessibility and effectiveness of the remedies in the different Member States.

Utrecht, 10 July 2006

[6] BVerfG, 1 BvR 518/02 , 4 April 2006.

Biography

Comments of the Standing Committee of experts in international immigration, refugee and criminal law on the draft proposal for a Regulation concerning the Visa Information System COM (2004) 835, CM 05-01, 29 April 2005, www.commissie-meijers.nl

Working Document on biometrics of the Article 29 Data Protection Working Group on biometrics, 1 August 2003, WP 80 http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup

Opinion of the European Data Protection Supervisor (EDPS) on the proposals for SIS II (the second-generation Schengen Information System, 19 October 2005.

Opinion the European Data Protection Supervisor (EDPS) on the proposal for a Council Framework Decision on principle of availability, 28 February 2006

Comments of the European Data Protection Supervisor (EDPS) on the Communication of the Commission on the interoperability of European databases, 10 March 2006

Opinion of the Article 29 Working Party on Data Protection on Regulation 2252/2004 on biometrics in passports and travel documents, 30 September 2005

Report of the Schengen Joint Supervisory Schengen Authority on an inspection on the use of Article 96 alerts in the Schengen Information System, Brussels, 20 June 2005, available at: www.statewatch.org.

Justice, *Comments on the EU Draft Council Framework Decision on the protection of personal data in the framework of police and judicial co-operation in criminal matters*, February 2006

Evelien Brouwer, *Data surveillance and border control in the EU: Balancing efficiency and legal protection of third country nationals* http://www.libertysecurity.org/article289.html