Statewatch analysis

From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained

by Ben Hayes
February 2004

Contents

Executive summary 3

Introduction, background and statistics on SIS operation 5

PART I: EXTENDING THE SCOPE OF THE SIS 7

New role for intelligence agencies
Access to SIS for vehicle registration authorities
Europol access to the SIS
Eurojust and national judicial authorities access to the SIS
New categories of data
Increased use of SIRENE
Data protection and storage limits
The legislation: has Poland stalled adoption of the measures?

PART II: THE DEVELOPMENT OF SIS II 17

Scope and function of SIS II
"Latent" technical development
No public debate: another cover-up?
Timetable for SIS II development

PART III: PROPOSED VISA INFORMATION SYSTEM 23

A "shared technical platform" …
but separate legal frameworks
The data to be held on VIS

CONCLUSION 27

Appendix 29

The 1990 Schengen Convention:
Proposed amendments to Title IV (Articles 92-119)

Executive summary

SIS II + VIS + PNR: Can Privacy and Free Movement Survive?

Law enforcement databases, it is said, are the product of "original sin". "Function creep" is inevitable, regardless of any assurances given by the executive at the time. The Schengen Information System was conceived in the mid 1980s to "compensate" for the removal of internal borders between France, Germany, Holland, Luxembourg and the Netherlands. Their police, intelligence, immigration and customs services, it was agreed at the time, had to be able to "alert" each other to be people refused admission (immigration offenders or security risks), people wanted for arrest, extradition or to testify in court, fugitives, persons to be placed under surveillance and stolen objects (vehicles, works of art, identity documents etc.).

And so it was that the SIS went online in March 1995 with the five original Schengen signatory states participating. By March 2003 and now under the auspices of the EU, the SIS covered 13 of the 15 EU member states, plus Norway and Iceland, who together had created records on 877,655 people, a further 386,402 aliases, and more than 15 million objects. EU officials estimate that there are 125,000 access terminals to the SIS. Under finalised proposals, access to the SIS is to be extended to Europol, Eurojust, national prosecutors and vehicle licensing authorities.

SIS II will allow the UK and Ireland and the ten accession states to participate in the SIS and, as expected, a host of new functions are planned. These include the addition of biometric identification data (photographs and fingerprints); new categories of "terrorist suspects" and "violent troublemakers" (who are to be banned from travelling to demonstrations or foot ball matches); and the linking of individual records. A second database - the Visa Information System (VIS) - is to share a "technical platform" with SIS II and will contain the extensive personal information supplied by people from around the world in an estimated 20 million visa applications to the EU member states every year. Like SIS II, VIS will contain biometric identification data.

Two years ago the European Commission acknowledged that "some of the proposals currently under discussion would fundamentally change the functions of the SIS, "transforming it from a reporting system to a reporting and investigation system". However, there has been no consultation of the European and national parliaments on the planned new functions. Instead, the member states and officials in the Council and Commission have conspired to avoid debate altogether and agreed to create the "technical capacity" for the new functions in SIS II and then "activate" them later on (so-called "latent development"). "Possible" new functions will be agreed in May in the form of EU Council conclusions and the Commission will appoint a contractor to develop the new system in August. This will present parliaments and civil society with a fait accompli and guarantee that "function creep" is built-in to the databases.

SIS II and VIS must be seen in a wider context. Firstly, there are global plans, promoted by the US and UK in various intergovernmental fora, to introduce biometrics in all travel documents (and the databases of the issuing authorities). Second, the 'PNR' (Passenger Name Record) scheme developed by the US to allow the pre-screening of all air travellers to the US will result in practise in the creation of detailed and lasting records on all entrants (in "CAPPS II"). The EU has agreed to US demands for European airlines to provide data on EU citizens despite the absence of an adequate data protection framework in the US, but more importantly, has proposed its own PNR scheme (see below).

Taken together, SIS II, VIS and PNR will introduce the surveillance of the movements of everyone in the EU - citizens, legally resident third-country nationals, visa entrants and irregular migrants - and the storage of their personal data on an unprecedented scale. John Lettice has explained how the:

> *current enthusiasm for profiling, the idea being to identify possible threats from people who aren't known, and have no record, absolutely requires broad data capture, use and retention. Course we've got to compile records on people who're innocent - otherwise, how could we confirm they're innocent? And anyway, innocent people have nothing to hide. Or they soon won't have… (1)*

And of course, it is the Muslims, the Arabs, migrants and refugees from the Third World who will suffer disproportionately - SIS II, VIS and PNR are designed to extend the "counter-terrorism" net. These systems will be used for speculative surveillance, general intelligence gathering and "fishing expeditions", but more importantly, individual records will increasingly result in coercive sanctions, such as the refusal to travel, the refusal of visa or asylum applications, the refusal of admission to a country at external borders, detention pending extradition, even deportation. Moreover, the massive sharing of data between the EU, US and other wealthy nations could provide for a kind of informal "mutual recognition" of these sanctions, where a (potentially arbitrary) decision taken by one country is then enforced by all the others.

In the longer term, EU-US cooperation heralds a global identification system, the global surveillance of movement and a global police information system - what place "free movement" and privacy in this scenario?

Ben Hayes, February 2004

Note (1) "Got a ticket? Get a record", by John Lettice, from *TheRegister.co.uk*, 3.2.04 (http://www.theregister.co.uk/content/6/35314.html)

See also *Statewatch's* Observatories on PNR and US and Observatory on EU PNR scheme (http://www.statewatch.org/observatories.htm)

From the Schengen Information System to SIS II and the Visa Information System (VIS): the proposals explained

INTRODUCTION

The Schengen Information System (SIS), the database used by the EU member states to record the details of millions of people and items of interest to police, customs and immigration authorities is to be extended under finalised proposals in the Council of the European Union. More agencies will have access and new types of data will be collected and stored.

At the same time, plans for SIS II, the 'second generation' SIS, and a new database –the Visa Information System (VIS) which will share a technical platform with SIS II – are developing rapidly, albeit outside the 'normal' EU decision-making process. This report explains the changes to SIS and the plans for SIS II/VIS.

Background

The 1985 Schengen Agreement created an elaborate security framework to 'compensate' for the removal of internal border controls among participating states. It covers immigration, asylum and visa policy as well as police and judicial cooperation. The Amsterdam Treaty integrated the Schengen framework into that of the EU producing a hugely complex legal system.

The Schengen Information System (SIS), has been operational since March 1995 and now covers 13 of the 15 EU countries, plus Norway and Iceland - the UK and Ireland are the only member states not yet participating, though plans to incorporate them and the accession states are well underway (though because of the UK's insistence on maintaining its own border controls they will not be able to create or access immigration and asylum related records).

Member states contribute data to the SIS on people wanted for arrest; people to be placed under surveillance or subject to specific checks; people to be refused entry at external borders (on either national security, including public order, or immigration grounds); and lost or stolen items. It currently contains over 15 million records, most of which relate to stolen items (see below); agencies can only access relevant categories of data.

Statistics on the operation of the SIS were produced every year in an annual report on the implementation of the 1990 Schengen Implementation Convention. However, with the incorporation of the Schengen structure into the EU/EC framework under the 1997 Amsterdam Treaty, the Council General Secretariat took an arbitrary 'informal' decision to discontinue the annual report (see *Statewatch News online*, March 2001). The last of the

annual reports was produced in November 1999, though *Statewatch* has managed to obtain more up-to-date figures:

1995: 3,868,529

1996: 4,592,949

1997: 5,592,240

1998: 8,826,856 (5.3.98)

2000: 9,748,083 (23.5.00)

2001: 14,476,665 (Council estimate for end of 2001)

2003: 877,655 wanted persons in total plus 386,402 aliases (5.3.03):

- *article 95:* 14,023 [arrest/extradition]

- *article 96:* 780,922 [to be refused entry (mostly rejected asylum-seekers but including those to be refused entry on grounds of "national security" and "public order")]

- *article 97:* 32,211 [missing/dangerous persons]

- *article 98:* 34,413 [wanted to appear in court]

- *article 99:* 16,016 [discreet surveillance]

Plans to develop a 'second generation' SIS have been happening since the late 1990s. Documents published on the *Statewatch* website in March 2002 (see *Statewatch News online*) outlined a host of far-reaching proposals for SIS II, some on which there was "general agreement", and others requiring "further discussion". Three months later a number of these proposals were put into formal draft EU decisions to amend the Schengen Convention and extend the capabilities of the existing SIS. These have now been finalised and are awaiting adoption by the Council of the European Union.

Meanwhile, discussions on the scope and function of the next-generation *SIS II* have proceeded in almost total secrecy . This is because the Council (EU governments) has decided to return to the controversial legal and political issues at a later date, *after* the contracts have been awarded and technical development of the new system are underway – allowing for what it calls the "latent" development of SIS II:

> *meaning that the technical pre-conditions for such functions should be available in SIS II from the start, but those functions would only be activated once the political and legal arrangements were in place [6387/02, 25.2.03].*

PART I: EXTENDING THE SCOPE OF THE EXISTING SIS

Rules on access to the current SIS are set out in Article 101:

> *Access to data included in the Schengen Information System and the right to search such data directly shall be reserved exclusively for the authorities responsible for*
> *(a) border checks;*
> *(b) other police and customs checks carried out within the country, and the coordination of such checks.*

In March 2003, there were – according to an EU report - "approximately 125,000!!!" [sic] terminals with access to the SIS (up from 55,000 access point in 1999) – so many that EU officials can only estimate. Any supposed restrictions on access are therefore very difficult to verify in practise. Under the current proposals, access to the SIS is to be extended to Europol, Eurojust, national prosecutors, and, it would seem, the national intelligence and security agencies of the member states.

New role for intelligence agencies

Article 99 of the 1990 Schengen Implementing Convention allows people to be entered on the SIS for the purposes of "discreet surveillance and specific checks" where:

> *there are real indications to suggest that the person concerned intends to commit or is committing numerous and extremely serious offences, or … will commit [them] in the future (Article 99(2))*

Police, customs and immigration officers in every member state are then alerted by the SIS to collect and report certain categories of information (see Article 99(4)) on the people concerned. The "authorities responsible for State security" – the intelligence and internal security agencies – may also have records entered "on their behalf" under Article 99, but only where:

> *concrete evidence gives reason to suppose that [it] is necessary for the prevention of a serious threat by the person concerned or other serious threats to internal or external security*

with a requirement to

> *consult the other [member states] beforehand (Article 99(3))*

The result is that the intelligence and security agencies have not directly entered anyone on the SIS under Article 99(3) since it went online in 1995 – whereas 16,016 people have been registered under article 99(2) by (police) criminal intelligence agencies. There is an obvious reluctance on the part of the security agencies to divulge intelligence on who they want placed under surveillance and why.

An amended Article 99(3) will remove the obligation on the intelligence agencies to inform the other member states beforehand when placing someone under surveillance. In doing so, the "concrete evidence" requirement may be circumvented in practise because of the effective supremacy of "national security" considerations. As the Spanish delegation puts it:

> *In any case, in the event of a hit, the Sirene Bureau of the country issuing the alert can be obliged to give details of the reasons for entering the alert in SIS, and even if the authorities responsible for State security were reluctant to give the Sirene Bureaux certain explanations for fear that an operation might miscarry, they could at least inform their own counterpart in the country in which the hit was made [6307/1/02, 18.2.02]*

Last year's proposals to give intelligence and security agencies access to the SIS were accompanied by a UK proposal to create a dedicated database of "terrorist suspects". It appeared that neither were included the subsequent proposals to extend the SIS that are currently on the table. This was strange since the presidency had described access for the intelligence services as being proposed:

> *with a view to reaching an agreement as soon as possible and implementing them quickly [5696/02, 5.2.02]*

Statewatch has tracked the proposal through the EU Working Party on the SIS. The discussions suggest that the proposal has been agreed and implemented "informally" – without a formal Council decision or consultation of the European and national parliaments.

The initial proposals had suggested that:

> *Within several [member states] security or intelligence services have a statutory or defined responsibility to combat terrorism and several share this responsibility with police services. The role of the "authorities responsible for State security" is already recognised within the Schengen Convention with Article 99(3) providing for alerts issued on their behalf… the Belgian Presidency highlighted the importance of defining "those authorities responsible for State Security".*
>
> *In the absence of such a definition it is the intention of these proposals to apply to those Security and Intelligence Services with internal security responsibilities allied to Justice or Home Affairs / Interior Ministries as opposed to military or other intelligence services with external responsibilities. [5696/02, 5.2.02]*

A week later, minutes of the SIS Working Party recorded:

> *general agreement on the proposal that access to the SIS could be given to those services which, according to national legislation, have a responsibility to combat terrorism. In accordance with the obligation of Article 101(4), each State would then have to give a detailed list of which authorities are covered by this definition. [6386/02, 15.2.02]*

This was subject to a scrutiny reservation from one of the member states (though the name of the country is blanked out in the documents). Its position was restated two months later on the basis of concern over "access to the SIS for non-police organizations" and "security and intelligence services not belonging to a police service" [7939/02, 15.4.02]. The last recorded discussion of the issue in the SIS Working Party is in May 2002:

> *The Chairman informed the meeting that the Presidency of the Terrorism WG had explained that his WP was in favour of providing SIS access for security and intelligence services. This would thus have to be* ***implemented at national level****. (emphasis added)*

So there we have it: an informal decision at working party level has extended access to the SIS to EU intelligence and security services which can simply be implemented at the national level. This raises a number of legal and political issues.

The last publicly available report concerning Article 101(4), under which each State must provide a detailed list of which authorities have access to which data, was produced almost 3 years ago [5002/2/00, 25.10.00]. How long will it be until the member states next make this information publicly available?

If access to the security services is granted on the basis of shared "responsibility to combat terrorism" with the police, what categories of data will the security and intelligence services have access to? The initial proposals suggested "all SIS data". For what purposes can they use this data and how will the data protection provisions be applied?

Finally, as it has been decided that intelligence and security services should have access to the SIS, this should surely be stated in a formal amendment of the Schengen Convention.

Access to SIS for vehicle registration authorities

Access for vehicle registration authorities to the data stored in the SIS (under Article 101(1)(b)) was first proposed in mid-1999 and could also, at least in some member states, have been decided and implemented in the same, informal way. Norway, for example, has

> *the opportunity to have these vehicles checked against the SIS as they are being cleared through Customs. Access to the SIS by*

Customs is covered by the convention and accordingly only needs a national decision [12803/99,10.11.99].

However, a proposal from the European Commission to regulate vehicle registration authorities' access the SIS was produced last August [COM (2003) 510, 21.8.03]. Access to the SIS for the intelligence services, on the other hand, is unlikely to be formalised until SIS II is developed (see below), if indeed their access is to be regulated at all.

Europol access to the SIS

Proposals to give Europol access to the SIS first appeared as a recommendation in the EU "Action Plan on Organised Crime" of 21 June 1999 (rec. no. 36), and later in proposals to extend the SIS to combat "terrorism". Europol put its case to the member states in the Council in February 2002, arguing access to the SIS was a strategic necessity (see *Statewatch news Online*, March 2002):

-Strategic analysis is of unquestionable interest to Europol and allows forecasts to be made using the following techniques:

- Identifying and comparing changes in different levels of crime over a period of time.

- Identifying possible relationships between relevant variables which have an impact on the crime rate.

- Comparing ethnic and demographic trends [5970/02]

Europol requested "immediate" access to "all information in the SIS" together with a facility for "Partial downloading of data in order to carry out analyses and statistical studies". In the longer term, Europol wants the member states to allow for the

Possibility of [Europol] updating SIS by adding, deleting and modifying information.

What the member states are set agree in the current proposals is Europol

access to, and [the right] to search directly, data entered into the Schengen Information System in accordance with Articles 95, 99 and 100 (proposed new Article 101 A)

This covers:

- persons wanted for arrest for the purpose of extradition [Article 95, 14,023 records in March 2003];

- persons to be subjected to discrete surveillance and specific checks [Article 99, 16,016 records in March 2003];

- objects sought for the purposes of seizure or of evidence in criminal proceedings: motor vehicles, boats and aircraft, trailers, caravans, industrial equipment, outboard engines and containers; firearms, blank official documents, issued identity papers such as passports, identity cards, driving licences, residence permits and travel documents, vehicle registration certificates and number plates, banknotes, securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated or lost [revised Article 100; 15 million records].

The legitimacy of this Decision rests on a rather weak argument that through Europol, the member states will make more "efficient" use of the SIS, though it is clear that Europol wants access for intelligence rather than law enforcement purposes:

The general purpose of the Schengen Information System is to maintain public order and security…

Regarding the usage limitation set out in the Articles 95 – 100 for each of the categories of reports and data, it is clear that Europol can not fulfil these requirements…

The usage of the reports and/or the data can therefore only be legitimised given the nature of Europol as an information broker.

As explained earlier the main goal for Europol's having access to SIS data is the cross-checking of information and the eventual input of relevant data in Europol's databases after a formal approval from the Reporting Contracting Party. [9323/02, 28.5.02]

There was in fact outright opposition to Europol access from several member states – including France [5495/00, 19.1.00] and later the Belgian delegation, which:

wonders about Europol's reasons for seeking entitlement to consult the SIS... Europol wishes to use the SIS on the basis of its own analysis work. However, Europol and the SIS have different goals. In the present circumstances, giving Europol access on the basis of the arguments in the above text is out of the question. [6890/02, 5.3.02]

This opposition has been overcome and the only restrictions on Europol's access is to that under Articles 96 (persons to be refused entry to the EU on national security, public order or immigration grounds – 780,922 records in March 2003) and Article 97 (missing or dangerous persons; 32,211 records). Nor will Europol be able to download whole sections of the SIS as it had hoped – though this is clearly prohibited by Article 101(2) anyway. But, with the consent of the member state who entered the data, Europol will be able to add the information on the SIS to its own extensive database, and

exchange it with various non-EU states and agencies with which cooperation agreements are in force.

Eurojust and national judicial authorities access to the SIS

Under the proposals on the table, Eurojust, the fledgling EU prosecutions agency, will also have access to the SIS. This is no less contentious. A Declaration attached to the Council Decision setting up Eurojust stated that:

> *The Council agrees to adopt, as a matter of urgency and in accordance with the principles laid down in Article 101 (3) of the Schengen Convention, no later than 15 June 2002, arrangements whereby the national members of Eurojust will have access to certain data in the Schengen Information System, in particular those referred to in Article 95 and 98 of the Schengen Convention. [OJ 2002 L 63/1]*

Like Europol, Eurojust actually wanted access to all the data on the SIS [11653/02, 30.7.02] and to be able to consult the Sirene bureaux directly (see below), arguing that:

> *wherever access to the SIS is useful in a domestic or international context in the course of an investigation or prosecution it will inevitably be useful to the National Members of Eurojust in co-ordinating such investigations and or prosecutions. [13389/02, 22.10.02]*

Again, there with was significant opposition, with Belgium arguing that:

> *Several fundamental issues arise… to what extent does Eurojust genuinely need this information to perform its tasks? Where do the interest and dangers of such consultation lie, given that the SIS is a system for checks and alerts, and not one that has been developed to underpin judicial investigations?*
>
> *Fundamentally, we do not therefore consider it necessary, as things stand, to grant Eurojust the right to consult the SIS, even for information purposes. Nonetheless, despite these substantive objections - which might be withdrawn once the parties concerned provide justification - a Council Declaration does in fact state that the national members of Eurojust must indeed have access to the SIS. Belgium cannot therefore categorically oppose such a possibility for consultation…*
>
> *A change in attitude might be considered in due course only on the basis of genuine justification from Eurojust [14037/02, 8.11.02]*

Aside from the question of why Belgium signed a declaration to which it was "fundamentally" opposed (though this perhaps offers a salutary lesson in the nature of EU decision-making), no further "justification" from Eurojust has

been forthcoming. Regardless, agreement is pending on Eurojust access to the data Articles 95 and 98 (proposed new Article 101B). However, where Europol will have the right to search the SIS "directly",

> *The national members of Eurojust and their assistants shall have the right to have access to, and search, data..*

There is no explanation for the different wording, though with the proposal agreed at working party level (see below), it maybe this issue that is preventing the adoption of the Decision. In a statement to be annexed to the finally adopted decision:

> *Germany would point out that national members of Eurojust and their assistants, when carrying out their work for Eurojust, are not subject to national law but only to the Eurojust Decision. The technical arrangements for access to the SIS by national members of Eurojust must therefore be determined by the Council. Germany proposes that a technical access model be developed that is similar to that chosen for the partial participation of the United Kingdom and Ireland in the SIS.*
>
> *Germany would point out that the different wordings used in Article 101a(1) and 101b(1), under which only Europol is to have the right to search SIS data "directly", do not necessarily mean that no provision may be made for direct access by Eurojust (for the national members of Eurojust and their assistants)*
> *[10056/03 ADD 1, 16.6.03]*

With such a discrepancy in the wording of the proposal and its actual intent, and the serious questions regarding the judicial control of Eurojust, it is astonishing that the Council considers the text ready for adoption [10056/03, 4.6.03 and 10056/03, ADD 1, 16.6.03].

The proposals on Europol and Eurojust access also ignore the draft cooperation agreement between the two agencies that will allow the sharing of data [15829/03, 9.12.03]. In practise, access for the two agencies may be complementary, allowing Europol and Eurojust to search all the data in the SIS between them in connection with specific investigations (except for that held under Article 96).

Another addition to Article 101, extends access to the SIS to:

> *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.*

Here there are no restrictions on which categories of data may be searched – this will apparently be determined by the member states. This is another significant extension of the function of the SIS and given Eurojust's

relationship with national judicial authorities (through the Eurojust "college", European Judicial Network or in joint investigation teams) will potentially extend access by EU agencies.

Access for immigration officers, visa authorities and asylum adjudicators will also be extended, from persons to be refused entry (Article 96) to false, stolen or lost identity documents (Article 100(3)(d) and (e)) under a revised Article 101(2).

New categories of data

Article 99 will also be widened to allow not just the entry of persons and vehicles on the SIS, but boats, aircrafts and containers. Objects sought for seizure or evidence in relation to criminal proceedings (Article 100) is widened to include boats, aircraft, industrial equipment, outboard engines, containers, invalidated identity papers (as well as lost or stolen ones), cheques, credit cards, stocks and shares.

Article 95 of the SIS covers persons wanted for arrest for extradition. The European Arrest Warrant will replace extradition requests, though the EAW will continue to be issued on the SIS through alerts under Article 95. The data held in the SIS under this category will be widened to include the offence that the person is wanted for.

Increased use of SIRENE

Behind the SIS is a network of national contact points called SIRENE (Supplementary Information Request at the National Entry). Each participating member state has a "Sirene Bureau" which is responsible for giving access to detailed information following a 'hit' on the SIS. There is no effective limit on the data that can be exchanged through the Sirene bureaux. There were at least 35,414 hits (requests for additional, detailed information) in 2001, the most recent year for which figures are readily available [12150/02, 2.10.02].

A new Article 92(4) refers to the Sirene bureaux in Schengen Implementing Convention for the first time (the network was developed in the Schengen working parties and the Schengen member states' Executive Committee):

> *Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (SIRENE) all supplementary information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System.*

The only restrictions on SIRENE are that "Such information shall be used only for the purpose for which it was transmitted" (revised Article 92) and

that all information exchanged is to be deleted after one year (new Article 112A). However, how the use and deletion of this data can be supervised in practice is unclear, since much of it will have been passed from the national Sirene bureaux to the police or other agencies in that country.

Data protection and storage limits

The one welcome amendment in the proposal is that under a revised Article 103 every transmission of personal data will be recorded instead of every tenth one. This will at least mean that unlawful or warranted use of the SIS or supplementary exchange of data will be theoretically traceable. However, this modest improvement is likely to be of little benefit without additional resources for the Joint Supervisory Authority on data protection, a workable mechanism for individuals to find out whether information on them is held on the SIS and the power for the JSA or other independent body to investigate and remedy individual complaints.

A Revised Article 113 will see the time period that objects sought in connection with criminal proceedings can be included in the SIS increase from three to five years.

The legislation: has Poland stalled adoption of the measures?

The proposals to amend the Schengen Convention provisions on the SIS take the form of a draft EU Council Decision and a draft EC Regulation. Scrutiny reserves by the member states were withdrawn in June 2003 and the proposals were both apparently agreed at Working Party level. However, in July 2003 came an unprecedented intervention by the Polish delegation requesting "consultation" on the draft Decision. Like Germany, Poland questioned the different wording regarding Europol and Eurojust access to the SIS (see above):

> *Poland is not aware of the reasons that lie behind the differentiation of the access to SIS granted to Europol and to Eurojust… Poland is of the opinion that full access to data [for Eurojust] regarding the criminal proceedings is necessary [13909/03, 10.7.03]*

Following the conclusion of the accession negotiations, the countries joining the EU are consulted on all documents submitted to Coreper and the Council. If one of the ten acceding countries is unhappy with any of the texts being adopted, it can request consultations within an interim Committee [11309/03, 10.7.03]. The Interim Committee met at least ten times during 2003 but the minutes of these meetings have not been made available to the public.

Main sources:

Draft Council Decision concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, 10054/03, 24.6.03; Draft Council Regulation concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism 10055/03, 24.6.03

Statewatch has incorporated the proposals into a revised Title IV of the 1990 Schengen Implementing Convention (see Appendix)

PART II: THE DEVELOPMENT OF SIS II

The Schengen Executive took the decision to create SIS II in late 1996 after Italy, Austria and Greece joined the SIS. This took the number of participating state to ten – two more than originally planned – and with the prospect of up to 25 countries eventually joining it was agreed that the existing SIS simply could not cope (the European Commission has recently said that the capacity of the SIS is 18 countries).

An opportunity to build new functions into SIS II was always going to be very tempting and it appears that discussions began soon after. There was nothing on the new functions for SIS II in the public domain, however, until 2000, and only then when *Statewatch* published and analysed EU Council working party documents. Discussions have since proceeded in almost total secrecy, though the case for an wider SIS II was made after 11 September 2001 that:

> *When the SIS was first created, its only purpose was to be a compensatory measure for the opening of the borders. Ever since, and not in the least because the SIS has proven to be a useful and efficient tool, recognition has grown that the potential of the SIS could be maximised… the idea of using the SIS data for other purposes than those initially foreseen, and especially for police information purposes in a broad sense, is now widely agreed upon and follows from the Council conclusions after the events of September 11 2001*

By the end of 2001, EU Justice and Home Affairs Ministers had agreed on funding the development of SIS II from the Community budget [Regulation 2424/2001, OJ 2001 L 328/4; Decision 2001/886/JHA, OJ 2001 L 328/1]. At the same time, a communication on SIS II was produced by the European Commission. It was under no illusions about the effect of the proposals being discussed by the member states:

> *some of the proposals currently under discussion would fundamentally change the functions of the SIS, transforming it* ***from a reporting system to a reporting and investigation system*** *[emphasis added. COM 2001 720, 18.12.01]*

However, the Commission stopped far short of calling for public debate or the full involvement of the European and national parliaments in the decision-making process. Meanwhile, its SIS II project team had already prepared the terms of a feasibility study to:

> *give an overview of the full potential scope for a new SIS. This does not pre-empt the fact that the discussion on new requirements is still on-going in the Council framework and could be further developed, but it provides the necessary basis in order to avoid a narrow description that would lead to a less capable solution, in terms of handling future changes. The requirements on a future SIS*

define the now known "outer limits" for what the SIS II, as a technical infrastructure, must be able to handle. [11527/1/01, 30.11.01]

With the presumably favourable feasibility study now completed (needless to say it has not been published) technical development of SIS II will begin later this year once the contract has been awarded (the call for tender went out in August 2003).

Scope and function of SIS II

Conclusions of the EU Justice and Home Affairs Ministers in May 2003 [9808/03, 26.5.03] split the proposals for new functions and types of data for SIS II into three categories: (a) those on which there is full agreement, (b) those subject to "full to wide-ranging agreement" and (c) those on which "a certain interest exists".

(a) SIS II, "must allow" for:

- the addition of new categories of alerts, both on persons and on objects (including where necessary the possibility that certain alerts be automatically deleted after a certain event/date);

- the inter-linking of any alerts, ensuring that this does not change the existing access rights to the different categories of alerts;

- the addition of new fields in the alerts and the modification of existing fields (including changing the optional character of a field to mandatory or vice versa);

- the modification of the duration of the alerts;

- new authorities to get access to the SIS (including where necessary the possibility to give partial access or access with a purpose different from the original one set in the alerts);

- the storage, transfer and possible querying of biometric data, especially photographs and fingerprints.

(b) There is "full to wide-ranging agreement" on:

- the list of what links can exist between which types of alerts;

- which fields will be included and/or modified in alerts on issued documents;

- which additional information and/or fields, if any, will be included in (certain) alerts;

- the (practical) conditions for storing photographs and fingerprints on wanted persons;

These should be:

implemented in the first release of SIS II.

(c) Finally, "a certain interest exists on the following proposals", though these require "further discussion":

- how, in view of the conclusions of Tampere and of the EU action plan to combat terrorism, should the purpose of the system be changed or extended, and notably:

· which authorities should acquire (an extended) access to the SIS and what purpose they can use this access for: the study should include the possibility for some authorities to use the SIS data for purposes other than those for which they were originally introduced in the SIS

· the legislative implications this might have, most importantly concerning data protection

· the technical impact this might have (including that at the national level)

· the need for ensuring that the efficiency of the current system is maintained and improved;

- which new categories of persons should be introduced in the SIS, and notably:

· minors precluded from leaving the Schengen area

· violent troublemakers;

- which new categories of objects should be introduced in the SIS under Articles 99 and/or 100, and notably

· other vehicles

· works of art

· animals

· luxury items

· any easily identifiable objects;

- which, if any, of the SIRENE forms must be included in the SIS database;

- what other biometric data can be stored in the SIS and what use, if any, can be made of the biometric data stored in the SIS;

- what intelligence use, if any, can be made of the records made according to Article 103;

- what modifications, if any, are necessary regarding the period an alert can be kept in the SIS;

- what data should be recorded under Article 103.

For an analysis of some of these proposals see *Statewatch bulletin* (vol 11 no 1, Jan-Feb 2001) and *Statewatch News Online* (November 2001, April 2002).

"Latent" technical development

It is clear that the member states are far from actual agreement over the more contentious proposals in (b) and (c) above. However, SIS II will be developed with the technical capacity for these functions anyway:

the technical specifications of the call for tender for SIS II shall respect the above conclusions.

The call for tender went out in August 2003. As for the legal and political issues:

in due time, the necessary legislative provisions reflecting the principles underlaying the current conclusions [will] be prepared for adoption.

This allows for what the SIS working party has called the "latent" development of SIS II:

the technical pre-conditions for such functions should be available in SIS II from the start, but those functions would only be activated once the political and legal arrangements were in place [6387/02, 25.2.03].

The contract for the "detailed design and development of SIS II" will be awarded in June 2004. This will be just after the Council agrees on the new functionalities – also scheduled for June 2004 – offering the European and national Parliaments, Joint Supervisory Authority on data protection (JSA) and civil society groups no chance to debate the serious civil liberties issues that arise.

No public debate: another cover-up?

It is the European Commission that has the legal mandate for the development of the actual SIS II system [Regulation 2424/2001/EC], though overall responsibilities are "shared" with the Council (member states). In practice, however, the Council retains control over all the key areas, describing its own competences in January 2004 – apparently in response to the Commission Communication of December 2003 – as follows:

- Legal description of the architecture of the system
- The definition of the categories of data…, the purposes for which they are to be entered and the criteria for their entry
- The contents of SIS records
- The definition of the authorities having access to SIS data
- The determination of the duration of SIS alerts
- The decision as to whether there should be a common type of N/SIS or a common type of interface to national systems
- Rules on interlinking of alerts
- Rules on compatibility between alerts
- Rules of responsibility for the correctness of alerts
- Rules on access by interested parties to SIS data
- Rules on the protection of personal data and their control
- Rules on security [5117/04 of 7.1.04]

The Commission is apparently left to find a contractor, sign the cheques and "tow the line". This has had a detrimental affect on the prospects for open and democratic debate on the development of SIS II. In its Communication on SIS II [COM (2003) 771, 11.12.03], with the exception of the use of biometrics data and the linking of alerts, the Commission makes no mention of the detailed Council proposals for SIS II outlined above – except to say that agreement is important before the contract is signed! Given that this Communication represents the only public summary of the development and SIS II, not to mention being the only "progress report" that the European Parliament receives, this omission is astonishing.

In an earlier communication on SIS II [COM (2001) 720, 18.12.2001], the Commission stated that the "European Parliament will be kept informed" and that "the Schengen Joint Supervisory Authority will have a role to play". In practice, however, the EP has been kept in the dark, forced into a draft recommendation to the Council calling for a "public debate" [2003/2180(INI), 20.11.03] and the JSA, similarly, having to request the Presidency to propose a Council declaration "stressing the need to involve the JSA in the development of the SIS II" [SCHAC 2506/03 & 2508/03].

By the time there is any public or "democratic" debate on the scope and function of SIS II, the technical requirements will be in place, it will doubtless be a "waste" not to use them, and the new system will effectively be a *fait accompli*.

Timetable for SIS II development

> *June 2003 – Definite list of functionalities and decision on the architecture [document not publicly available],*
>
> *August 2003 - Launch of the call for tender of SIS II,*
>
> *Mid-May – June 2004 – Final agreement of functions and presentation to [Article 36 Committee], Council Conclusions as required,*
>
> *June 2004 – Signature of the contract for the detailed design and the development of SIS II and subsequent draft of the detailed design,*
>
> *January 2005 – Start of SIS II development,*
>
> *Spring 2005 – Start of Schengen States/Member States national system adaptation,*
>
> *Autumn 2006 – Start migrating current Contracting Parties,*
>
> *End 2006 – Ready for integration of new Contracting Parties (the issue of whether acceding countries could integrate in parallel with present Parties is still under discussion).*

[6387/02, 25.2.03 and 5117/04 , 7.2.04]

PART III: THE PROPOSED VISA INFORMATION SYSTEM

In June 2002 the Council of the EU adopted guidelines (in the form of Council Conclusions) on the possible development of a Visa Information System – a database that would contain the personal information (including biometrics) on every visa application (irrespective of whether the visa was issued or the application refused). The proposal dates back to the aftermath of 11 September, when a host of new measures were proposed in the name of 'counter-terrorism'. However, the speed at which the German government came up with the initiative and the way it was received suggest the idea has been around for some time.

Another favourable feasibility study has been completed and the Commission has stated the purpose of the VIS system:

> *- facilitate the fight against fraud,*
> *- contribute to the improvement of consular co-operation and the exchange of information*
> *between central consular authorities,*
> *- facilitate checks at border checkpoints or at immigration or police checkpoints,*
> *- contribute to the prevention of "visa shopping",*
> *- facilitate the application of the Dublin Convention,*
> *- assist in the procedures for returning citizens of third countries,*
> *- contribute towards improving the administration of the common visa policy and internal security, and to combating terrorism [COM (2003) 771, 11.12.03].*

VIS would have a "capacity to connect at least 27 Member States, 12 000 VIS users and 3,500 consular posts worldwide". The study is based on the "assumption that 20 million visa requests would be handled annually".

There are three options for the inclusion of biometric data – iris scans, facial recognition and fingerprints, though discussions suggest that the EU will, like the US, opt for fingerprints.

A "shared technical platform" …

The Commission has proposed that:

> *VIS and SIS II could share a common business continuity system at the central level with a significant reduction of costs; both projects could be developed under a common management organisation which could have the oversight of the project implementation, …*
>
> *Apart from the obvious synergy advantages at central level, Member States can also achieve remarkable benefits and cost savings from synergy architecture.*

Thousands of end-users, which belong to police authorities, border control and immigration services, for example, could use SIS II equipment to check visa information via the future SIS II infrastructure. Additional investment for dedicated VIS equipment could be avoided and the daily work could be simplified and harmonised.

The Commission estimates that the costs of setting up the VIS database will be between 15 and 16 million euros, regardless of whether an independent or "common technical platform" with SIS II is pursued. The saving comes in the annual operational costs of an independent VIS database are estimated at 15 million euros; the Commission says that this would fall to 10 million if it shared a "common technical platform" with SIS II. To add "biometrics and supporting document functions" to the system will add a further 157-8 million euros to the investment costs with the annual operational budget estimated at 42 million euros.

… but separate legal frameworks

The Commission suggests that:

Since the new legal texts will have to be "Amsterdam-compatible", the development of SIS II is the appropriate occasion to present new legal texts to replace the entire Title IV of the Schengen Convention. This will also allow the European Parliament to play its full role as regards SIS II.

As regards the VIS, it goes without saying that despite the technical synergies, a separate legal framework will have to be established.

This is an inventive approach to the legislative and legal issues that arise in relation to SIS II and the VIS databases.

First, as suggested above, the European Parliament *will be excluded* from the decision on the technical specifications for SIS II which will almost certainly pre-empt debate on any new functions. Secondly, there is a strong possibility that any new regulatory framework will reserve "implementing powers" over the new databases to the Council (this has been the case with most key areas of JHA cooperation). In the draft EU constitutional treaty there is a clear attempt to exclude such matters from the "normal" legislative and regulatory processes.

Finally, the assertion that "it goes without saying that… a separate legal framework will have to be established" must be questioned. If the data in SIS II and the VIS system are to be stored on the same computer and, moreover, jointly accessible by "thousands of end-users", then there is surely a strong case for a single regulatory framework with a single data protection regime and supervisory authority.

The data to be held in the Visa Information System

According to draft Council Conclusions on the Visa Information System prepared in November [14766/03, 13.11.03], the "following information should be processed in the System in the first step":

> *(a) types of visa: Schengen uniform visas and Schengen "national visas", indicating types (A, B, C, D, D+C, including LTVs);*
>
> *(b) status of visas:*
> *- Visas requested*
> *- Visas issued,*
> *- Visas formally refused*
> *- Visas annulled, revoked, extended;*
>
> *(c) all the data required to identify the applicant, to be taken from the application form;*
>
> *(d) all the data required to identify the visa, to be derived from the sticker;*
>
> *(e) the competent authority that issued the visa (including border crossing points) and whether that authority issued it on behalf of another State, as well as the competent authority that formally refused, annulled, revoked or extended the visa;*
>
> *(f) standard grounds for refusing, cancelling, withdrawing and extending visas;*
>
> *(g) information obtained by the VISION consultation;*
>
> *(h) reference to supporting documents, when they are added to the visa file, and the authority where copies are stored, such as*
> *- travel documents*
> *- record of persons issuing invitations, those liable to pay board and lodging costs,*
> *- insurance policies;*
>
> *(i) process and status information; available in codes linked to a limited number of languages (English and French);*
>
> *(j) digitised photographs of the visa applicant.*
>
> *In a second step, in full coherence with the choice of biometric identifiers in the field of visas, biometric data on the visa applicants should be added to the VIS, thus allowing the linkage with the data mentioned above in point 2 for verification and identification purposes, including background checks.*

In a further step, the following supporting documents should be scanned and processed, when they are added to the visa file, such as
- travel documents,
- record of persons issuing invitations, those liable to pay board and lodging costs,
- insurance policies.

The draft conclusions also state that

The VIS will be based on a centralised architecture and a common technical platform with SIS II

which makes a mockery of the "options" for VIS set out in the Commission's communication. The conclusions also confirm that:

VIS-users should have access to consult SIS data via the Central Visa Information System (C-VIS), as far as they are entitled to consult the SIS

Finally, the Council suggests that data should be held for a period of at least ten years:

Data should remain in the system for on-line consultation for a period of five years. This period will start to run when the data of the decision on the visa application are entered in the system.

After the five-year period has elapsed,
- the VIS-data should be transferred to a central archive, available for off-line consultation, for a retention period of another five years;
- each Member State may decide to transfer the data to historical files, in accordance with its national legislation on data protection.

CONCLUSION

In 2002, the European Commission acknowledged that "some of the proposals currently under discussion would fundamentally change the functions of the SIS, "transforming it from a reporting system to a reporting and investigation system". However, there has been no consultation of the European and national parliaments on the planned new functions. Instead, the member states and officials in the Council and Commission have conspired to avoid debate altogether and agreed to create the "technical capacity" for the new functions in SIS II and then "activate" them later on (so-called "latent development"). "Possible" new functions will be agreed in May in the form of EU Council conclusions and the Commission will appoint a contractor to develop the new system in August. This will present parliaments and civil society with a fait accompli.

SIS II and VIS must be seen in a wider context. Firstly, there are global plans, promoted by the US and UK in various intergovernmental fora, to introduce biometrics in all travel documents (and the databases of the issuing authorities). Second, the 'PNR' (Passenger Name Record) scheme developed by the US to allow the pre-screening of all air travellers to the US will result in practise in the creation of detailed and lasting records on all entrants (in "CAPPS II"). The EU has agreed to US demands for European airlines to provide data on EU citizens despite the absence of an adequate data protection framework in the US, but more importantly, has proposed its own PNR scheme (see below).

Taken together, SIS II, VIS and PNR will introduce the surveillance of the movements of everyone in the EU - citizens, legally resident third-country nationals, visa entrants and irregular migrants - and the storage of their personal data on an unprecedented scale. John Lettice has explained how the:

> *current enthusiasm for profiling, the idea being to identify possible threats from people who aren't known, and have no record, absolutely requires broad data capture, use and retention. Course we've got to compile records on people who're innocent - otherwise, how could we confirm they're innocent? And anyway, innocent people have nothing to hide. Or they soon won't have… (1)*

And of course, it is the Muslims, the Arabs, migrants and refugees from the Third World who will suffer disproportionately - SIS II, VIS and PNR are designed to extend the "counter-terrorism" net. These systems will be used for speculative surveillance, general intelligence gathering and "fishing expeditions", but more importantly, individual records will increasingly result in coercive sanctions, such as the refusal to travel, the refusal of visa or asylum applications, the refusal of admission to a country at external borders, detention pending extradition, even deportation. Moreover, the massive sharing of data between the EU, US and other wealthy nations could provide for a kind of informal "mutual recognition" of these sanctions, where

a (potentially arbitrary) decision taken by one country is then enforced by all the others.

In the longer term, EU-US cooperation heralds a global identification system, the global surveillance of movement and a global police information system - what place "free movement" and privacy in this scenario?

References

Note 1. "Got a ticket? Get a record", by John Lettice, from The Register, 3.2.04 (http://www.theregister.co.uk/content/6/35314.html)

For a full list of references and links to the documents cited in this report see:

http://www.statewatch.org/semdoc/analysis/sources-sis-report.html

The 1990 Schengen Convention: Proposed amendments to Title IV (Articles 92-119)

This is text is potentially subject to further amendment. A final version of this document will be produced when the relevant proposals are adopted.

[Deleted text in ~~strikethrough~~, new text in *italics*]

TITLE IV

The Schengen Information System

CHAPTER 1

Setting up of the Schengen Information System

Article 92

1. The Contracting Parties shall set up and maintain a joint information system, hereinafter referred to as the Schengen Information System, consisting of a national section in each of the Contracting Parties and a technical support function. The Schengen Information System shall enable the authorities designated by the Contracting Parties, by means of an automated search procedure, to have access to reports on persons and objects for the purposes of border checks and controls and other police and customs checks carried out within the country in accordance with national law and, in the case of the single category of report referred to in Article 96, for the purposes of issuing visas, the issue of residence permits and the administration of aliens in the context of the application of the provisions of this Convention relating to the movement of persons.

2. Each Contracting Party shall set up and maintain, for its own, account and at its own risk, its national section of the Schengen Information System, the data file of which shall be made materially identical to the data files of the national sections of each of the other Contracting Parties using the technical support function. To ensure the rapid and effective transmission of data as referred to in paragraph 3, each Contracting Party shall observe, when creating its national section, the protocols and procedures which the Contracting Parties have jointly established for the technical support function. Each national section's data file shall be available for the purposes of automated search in the territory of each of the Contracting Parties. It shall not be possible to search the data files of other Contracting Parties' national sections.

3. The Contracting Parties shall set up and maintain jointly and with joint liability for risks, the technical support function of the Schengen Information System, the responsibility for which shall be assumed by the French Republic: the technical support function shall be located in Strasbourg. The technical support function shall comprise a data file which ensures that the data files of the national sections are kept identical by the on-line transmission of information. The data file of the technical support function shall contain reports on persons and objects where these concern all

the Contracting Parties. The data file of the technical support function shall contain no data other than those referred to in this paragraph and in Article 113(2).

4. Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (SIRENE) all supplementary information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System.

Such information shall be used only for the purpose for which it was transmitted.

CHAPTER 2

Operation and utilization of the Schengen Information System

Article 93

The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public order and security, including State security, and to apply the provisions of this Convention relating to the movement of persons, in the territories of the Contracting Parties, using information transmitted by the system.

Article 94

1. The Schengen Information System shall contain only the categories of data which are supplied by each of the Contracting Parties and are required for the purposes laid down in Articles 95 to 100. The Contracting Party providing a report shall determine whether the importance of the case warrants the inclusion of the report in the Schengen Information System.

2. The categories of data shall be as follows:

(a) persons reported

~~(b) objects referred to in Article 100 and vehicles referred to in Article 99.~~

(b) objects referred to in Articles 99 and 100.

~~3. The items included in respect of persons, shall be no more than the following:~~

~~(a) name and forename, any aliases possibly registered separately;~~

~~(b) any particular objective and permanent physical features;~~

~~(c) first letter of second forename;~~

~~(d) date and place of birth;~~

~~(e) sex;~~

~~(f) nationality;~~

~~(g) whether the persons concerned are armed;~~

~~(h) whether the persons concerned are violent;~~

~~(i) reason for the report;~~

~~(j) action to be taken.~~

3. For persons, the information shall be no more than the following:

(a) surname and forenames, any aliases possibly entered separately;

(b) any specific objective physical characteristics not subject to change;

(c) (...);

(d) place and date of birth;

(e) sex;

(f) nationality;

(g) whether the persons concerned are armed, violent or have escaped;

(h) reason for the alert;

(i) action to be taken;

(j) in cases of alerts under Article 95: the type of offence(s)

Other references, in particular the data listed in Article 6, first sentence of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, shall not be authorized.

4. Insofar as a Contracting Party considers that a report in accordance with Articles 95, 97 or 99 is incompatible with its national law, its international obligations or essential national interests, it may subsequently add to the report in the data file of the national section of the Schengen Information System a note to the effect that the action referred to will not be taken in its territory in connection with the report. Consultations must be held in this connection with the other Contracting Parties. If the reporting Contracting Party does not withdraw the report it will continue to apply in full for the other Contracting Parties.

Article 95

1. Data relating to persons wanted for arrest for extradition purposes shall be included at the request of the Judicial authority of the requesting Contracting Party.

2. Prior to making a report, the reporting Contracting Party shall check whether the arrest is authorized by the national law of the requested Contracting Parties. If the reporting Contracting Party has doubts it must consult the other Contracting Parties concerned. The reporting Contracting Party shall send the requested Contracting Parties together with the report, by the swiftest means, the following essential information relating to the case:

(a) the authority which issued the request for arrest;

(b) whether there is an arrest warrant or a document having the same force, or an enforceable Judgment;

(c) the nature and legal classification of the offence;

(d) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the person reported;

(e) as far as possible, the consequences of the offence.

3. A requested Contracting Party may add to the report in the file of the national section of the Schengen Information System a note prohibiting arrest in connection with the report, until such time as the note is deleted. The note shall be deleted no later than 24 hours after the report is included, unless the Contracting Party refuses to make the requested arrest on legal grounds or for special reasons of expediency. Where, in particularly exceptional cases, this is justified by the complexity of the facts underlying the report, the above time limit may be extended to one week. Without prejudice to a qualifying note or a decision to refuse arrest, the other Contracting Parties may make the arrest requested in the report.

4. If, for particularly urgent reasons, a Contracting Party requests an immediate search, the Party requested shall examine whether it is able to withdraw its note. The Contracting Party requested shall take the necessary steps to ensure that the action to be taken can be carried out without delay if the report is validated.

5. If the arrest cannot be made because an investigation has not been completed or owing to a refusal by the requested Contracting Party, the latter must regard the report as being a report for the purposes of communicating the place of residence of the person concerned.

6. The requested Contracting Parties shall carry out the action to be taken as requested in the report in compliance with extradition Conventions in force and with national law. They shall not be required to carry out the action requested where one of their nationals is involved, without prejudice to the possibility of making the arrest in accordance with national law.

Article 96

1. Data relating to aliens who are reported for the purposes of being refused entry shall be included on the basis of a national report resulting from decisions taken, in

compliance with the rules of procedure laid down by national legislation, by the administrative authorities or courts responsible.

2. Decisions may be based on a threat to public order or national security and safety which the presence of an alien in national territory may pose.

Such may in particular be the case with:

(a) an alien who has been convicted of an offence carrying a custodial sentence of at least one year;

(b) an alien who, there are serious grounds for believing, has committed serious offences, including those referred to in Article 71, or against whom there is genuine evidence of an intention to commit such offences in the territory of a Contracting Party.

3. Decisions may also be based on the fact that the alien has been the subject of a deportation, removal or expulsion measure which has not been rescinded or suspended, including or accompanied by a prohibition on entry or, where appropriate, residence, based on non-compliance with national regulations on the entry or residence of aliens.

Article 97

Data relating to persons who have disappeared or to persons who, in the interests of their own protection or in order to prevent threats, need to be placed provisionally in a place of safety at the request of the competent authority or the competent Judicial authority of the reporting Party, shall be included in order that the police authorities can communicate their whereabouts to the reporting Party or can remove the person to a place of safety for the purposes of preventing him from continuing his journey, if so authorized by national legislation. This shall apply in particular to minors and to persons who must be interned by decision of a competent authority. Communication of the information shall be subject to the consent of the person who has disappeared, if of full age.

Article 98

1. Data relating to witnesses, to persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or to persons who are to be notified of a criminal Judgment or of a summons to appear in order to serve a custodial sentence, shall be included, at the request of the competent Judicial authorities, for the purposes of communicating their place of residence or domicile.

2. Information requested shall be communicated to the requesting Party in accordance with national legislation and with the Conventions in force concerning mutual Judicial assistance in criminal matters.

Article 99

~~1. Data relating to persons or vehicles shall be included, in compliance with the national law of the reporting Contracting Party, for the purposes of discreet surveillance or specific checks, in accordance with paragraph 5.~~

1. Data on persons or vehicles, boats, aircraft and containers shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet surveillance or of specific checks in accordance with paragraph 5.

2. Such a report may be made for the purposes of prosecuting criminal offences and for the prevention of threats to public safety:

(a) where there are real indications to suggest that the person concerned intends to commit or is committing numerous and extremely serious offences, or

(b) where an overall evaluation of the person concerned, in particular on the basis of offences committed hitherto, gives reason to suppose that he will also commit extremely serious offences in future.

3. In addition, a report may be made in accordance with national law, at the request of the authorities responsible for State security, where concrete evidence gives reason to suppose that the information referred to in paragraph 4 is necessary for the prevention of a serious threat by the person concerned or other serious threats to internal or external State security. ~~The reporting Contracting Party shall be required to consult the other Contracting Parties beforehand.~~

The Member State issuing the alert pursuant to this paragraph shall be obliged to inform the other Member States thereof.

4. For the purposes of discreet surveillance, the following information may in whole or in part be collected and transmitted to the reporting authority when border checks or other police and customs checks are carried out within the country:

(a) the fact that the person reported or the vehicle reported has been found;

(b) the place, time or reason for the check;

(c) the route and destination of the journey;

(d) persons accompanying the person concerned or occupants of the vehicle;

(e) the vehicle used;

(f) objects carried;

(g) the circumstances under which the person or the vehicle was found.

When such information is collected, steps must be taken to ensure that the discreet nature of the surveillance is not jeopardized.

~~5. In the context of the specific checks referred to in paragraph 1, persons, vehicles and objects carried may be searched in accordance with national law, in order to achieve the purpose referred to in paragraphs 2 and 3.~~

5. During the specific checks referred to in paragraph 1, persons, vehicles, boats, aircraft, containers and objects carried may be searched in accordance with national law for the purposes referred to in paragraphs 2 and 3.

If the specific check is not authorized in accordance with the law of a Contracting Party, it shall automatically be converted, for that Contracting Party, into discreet surveillance.

6. A requested Contracting Party may add to the report in the file of the national section of the Schengen Information System a note prohibiting, until the note is deleted, performance of the action to be taken pursuant to the report for the purposes of discreet surveillance or specific checks. The note must be deleted no later than 24 hours after the report has been included unless the Contracting Party refuses to take the action requested on legal grounds or for special reasons of expediency. Without prejudice to a qualifying note or a refusal decision, the other Contracting Parties may carry out the action requested in the report.

Article 100

1. Data relating to objects sought for the purposes of seizure or of evidence in criminal proceedings shall be included in the Schengen Information System.

2. If a search brings to light the existence of a report on an item which has been found, the authority noticing the report shall contact the reporting authority in order to agree on the requisite measures. For this purpose, personal data may also be transmitted in accordance with this Convention. The measures to be taken by the Contracting Party which found the object must comply with its national law.

~~3. The categories of object listed below shall be included:~~

~~(a) motor vehicles with a capacity in excess of 50 cc which have been stolen, misappropriated or lost;~~

~~(b) trailers and caravans with an unladen weight in excess of 750 kg which have been stolen, misappropriated or lost;~~

~~(c) firearms which have been stolen, misappropriated or lost:~~

~~(d) blank documents which have been stolen, misappropriated or lost:~~

~~(e) identification documents issued (passports, identity cards, driving licences) which have been stolen, misappropriated or lost:~~

~~(f) bank notes (registered notes).~~

3. The following categories of readily identifiable objects shall be entered:

(a) motor vehicles with a cylinder capacity exceeding 50 cc, boats and aircraft which have been stolen, misappropriated or lost;

(b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers which have been stolen, misappropriated or lost;

(c) firearms which have been stolen, misappropriated or lost;

(d) blank official documents which have been stolen, misappropriated or lost;

(e) issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated;

(f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated;

(g) banknotes (registered notes);

(h) securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated or lost.

Article 101

1. Access to data included in the Schengen Information System and the right to search such data directly shall be reserved exclusively for the authorities responsible for

(a) border checks;

(b) other police and customs checks carried out within the country, and the coordination of such checks.

However, access to data entered in the Schengen Information System and the right to search such data directly may also be exercised by 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.

~~2. In addition, access to data included in accordance with Article 96 and the right to search such responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and the administration of aliens within the framework of the application of the provisions on the movement of persons under this Convention. Access to data shall be governed by the national law of each Contracting Party.~~

2. In addition, access to data entered in accordance with Article 96 and data concerning documents relating to persons entered in accordance with Article 100(3)(d) and (e) and the right to search such data directly may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation on aliens in the context of the application of the provisions of this Convention relating to the movement of persons. Access to data by these authorities shall be governed by the national law of each Member State.

3. Users may only search data which are necessary for the performance of their tasks.

4. Each of the Contracting Parties shall communicate to the Executive Committee a list of the competent authorities which are authorized to search the data included in the Schengen Information System directly. That list shall indicate for each authority the data which it may search, and for what purposes.

Article 101A

1. The European Police Office (Europol) shall within its mandate and at its own expense have the right to have access to, and to search directly, data entered into the Schengen Information System in accordance with Articles 95, 99 and 100.

2. Europol may only search data which it requires for the performance of its tasks.

3. Where a search by Europol reveals the existence of an alert in the Schengen Information System, Europol shall inform, via the channels defined by the Europol Convention, the Member State which issued the alert thereof.

4. Use of information obtained from a search in the Schengen Information System is subject to the consent of the Member State concerned. If the Member State allows the use of such information, the handling thereof shall be governed by the Europol Convention. Europol may only communicate such information to third States and third bodies with the consent of the Member State concerned.

5. Europol may request supplementary information from the Member State concerned in accordance with the provisions set out in the Europol Convention.

6. Europol shall:

(a) record every search made by it, in accordance with the provisions of Article 103;

(b) without prejudice to paragraphs 4 and 5, not connect parts of the Schengen Information System nor transfer the data contained therein to which it has access to any computer system for data collection and processing in operation by or at Europol nor download or otherwise copy any parts of the Schengen Information System;

(c) limit access to data entered into the Schengen Information System to specifically authorised staff of Europol;

(d) adopt and apply the measures provided for in Article 118;

(e) allow the Joint Supervisory Body, set up under Article 24 of the Europol Convention, to review the activities of Europol in the exercise of its right to accede to and to search data entered into the Schengen Information System.

Article 101B

1. The national members of Eurojust and their assistants shall have the right to have access to, and search, data entered in accordance with Articles 95 and 98 into the Schengen Information System.

2. The national members of Eurojust and their assistants may only search data which they require for the performance of their tasks.

3. Where a search by a national member of Eurojust reveals the existence of an alert in the Schengen Information System, he or she shall inform the Member State having issued the alert thereof. Any communication of information obtained from such a search may only be communicated to third States and third bodies with the consent of the Member State having issued the alert.

4. Nothing in this Article shall be interpreted as affecting the provisions of the Council Decision setting up Eurojust concerning data protection and the liability for any unauthorized or incorrect processing of such data by the national members of Eurojust or their assistants, or as affecting the powers of the Joint Supervisory Body set up pursuant to Article 23 of that Council Decision.

5. Every search made by a national member of Eurojust or an assistant shall be recorded in accordance with the provisions of Article 103 and every use made by them of data to which they have acceded shall be registered.

6. No parts of the Schengen Information System shall be connected nor shall the data contained therein to which the national members or their assistants have access be transferred to any computer system for data collection and processing in operation by or at Eurojust nor shall any parts of the Schengen Information System be downloaded.

7. The access to data entered into the Schengen Information System shall be limited to the national members and their assistants and not be extended to Eurojust staff.
8. Measures as provided for in Article 118 shall be adopted and applied.

CHAPTER 3

Protection of personal data and security of data under the Schengen Information System

Article 102

1. The Contracting Parties may use the data provided for in Articles 95 to 100 only for the purposes laid down for each type of report referred to in those Articles.

2. Data may be duplicated only for technical purposes, provided that such duplication is necessary for direct searching by the authorities referred to in Article 101.
Reports by other Contracting Parties may not be copied from the national section of the Schengen Information System in other national data files.

3. In connection with the types of report provided for in Articles 95 to 100 of this Convention, any derogation from paragraph 1 in order to change from one type of report to another must be justified by the need to prevent an imminent serious threat to public order and safety, for serious reasons of State security or for the purposes of preventing a serious offence. The prior authorization of the reporting Contracting Party must be obtained for this purpose.

4. Data may not be used for administrative purposes. ~~By way of derogation, data included in accordance with Article 96 may be used, in accordance with national law of each of the Contracting Parties, only for the purposes of Article 101(2).~~

By way of derogation, data entered under Article 96 and data concerning documents relating to persons entered under Article 100(3)(d) and (e) may be used in accordance with the national law of each Member State for the purposes of Article 101(2) only.

5. Any use of data which does not comply with paragraphs 1 to 4 shall be considered as a misuse in relation to the national law of each Contracting Party.

Article 103

~~Each Contracting Party shall ensure that, on average, every tenth transmission of personal data is recorded in the national section of the Schengen Information System by the data file managing authority for the purposes of checking the admissibility of searching. The recording may be used only for this purpose and shall be deleted after six months.~~

Each Member State shall ensure that every transmission of personal data is recorded in the national section of the Schengen Information System by the data file management authority for the purposes of checking whether the search is admissible or not. The record may only be used for this purpose and shall be deleted at the earliest after a period of one year and at the latest after a period of three years.

Article 104

1. The law applying to reports shall be the national law of the reporting Contracting Party, unless more rigorous conditions are laid down in this Convention.

2. Insofar as this Convention does not lay down specific provisions, the law of each Contracting Party shall apply to data included in the national section of the Schengen Information System.

3. Insofar as this Convention does not lay down specific provisions concerning performance of the action requested in the report, the national law of the Contracting

Party requested which carries out the action shall apply. Insofar as this Convention lays down specific provisions concerning performance of the action requested in the report, responsibility for the action to be taken shall be governed by the national law of the requested Contracting Party. If the action requested cannot be performed, the requested Contracting Party shall inform the reporting Contracting Party without delay.

Article 105

The reporting Contracting Party shall be responsible for the accuracy, up-to-dateness and lawfulness of the inclusion of data in the Schengen Information System.

Article 106

1. Only the reporting Contracting Party shall be authorized to amend, supplement, correct or delete data which it has introduced.

2. If one of the Contracting Parties which has not made the report has evidence to suggest that an item of data is legally or factually inaccurate, it shall advise the reporting Contracting Party thereof as soon as possible; the latter must check the communication and, if necessary, correct or delete the item in question without delay.

3. If the Contracting Parties are unable to reach agreement, the Contracting Party which did not generate the report shall submit the case to the joint supervisory authority referred to in Article 115(1) for its opinion.

Article 107

Where a person has already been the subject of a report in the Schengen Information System, a Contracting Party which introduces a further report shall come to an agreement on the inclusion of the reports with the Contracting Party which introduced the first report. The Contracting Parties may also adopt general provisions to this end.

Article 108

1. Each of the Contracting Parties shall designate an authority which shall have central responsibility for the national section of the Schengen Information System.

2. Each of the Contracting Parties shall make its reports via that authority.

3. The said authority shall be responsible for the correct operation of the national section of the Schengen Information System and shall take the measures necessary to ensure compliance with the provisions of this Convention.

4. The Contracting Parties shall inform one another, via the Depositary, of the authority referred to in paragraph 1.

Article 109

1. The right of any person to have access to data relating to him which are included in the Schengen Information System shall be exercised in accordance with the law of the Contracting Party before which it invokes that right. If the national law so provides, the national supervisory authority provided for in Article 114(1) shall decide whether information shall be communicated and by what procedures. A Contracting Party which has not made the report may communicate information concerning such data only if it has previously given the reporting Contracting Party an opportunity to state its position.

2. Communication of information to the person concerned shall be refused if it may undermine the performance of the legal task specified in the report, or in order to protect the rights and freedoms of others. It shall be refused in any event during the period of reporting for the purposes of discreet surveillance.

Article 110

Any person may have factually inaccurate data relating to him corrected or have legally Inaccurate data relating to him deleted.

Article 111

1. Any person may, in the territory of each Contracting Party, bring before the courts or the authority competent under national law an action to correct, delete or provide information or obtain compensation in connection with a report concerning him.

2. The Contracting Parties shall undertake amongst themselves to execute final decisions taken by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 116.

Article 112

1. Personal data included in the Schengen Information System for the purposes of locating persons shall be kept only for the time required to achieve the purposes for which they were supplied. No later than three years after their inclusion, the need for their retention must be reviewed by the reporting Contracting Party. This period shall be one year in the case of reports referred to in Article 99.

2. Each of the Contracting Parties shall, where appropriate, set shorter review periods in accordance with its national law.

3. The technical support function of the Schengen Information System shall automatically inform the Contracting Parties of a scheduled deletion of data from the system, giving one month's notice.

4. The reporting Contracting Party may, within the review period, decide to retain the report if its retention is necessary for the purposes for which the report was

made. Any extension of the report must be communicated to the technical support function. The provisions of paragraph 1 shall apply to report extension.

Article 112A

1. Personal data held in files by the authorities referred to in Article 92(4) as a result of information exchange pursuant to that paragraph, shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the alert or alerts concerning the person or object concerned have been deleted from the Schengen Information System.

2. Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period of time for which such data may be held in such files shall be governed by national law.

Article 113

~~1. Data other than those referred to in Article 112 shall be retained for a maximum of ten years, data relating to identity documents issued and to registered bank notes for a maximum of five years and those relating to motor vehicles, trailers and caravans for a maximum of three years.~~

1. Data other than that referred to in Article 112 shall be kept for a maximum of 10 years and data on objects referred to in Article 99(1) for a maximum of five years.

2. Data deleted shall continue to be retained for one year in the technical support function. During that period they may be consulted only for the purposes of subsequently checking their accuracy and the lawfulness of their inclusion. Afterwards they must be destroyed.

Article 113A

1. Data other than personal data held in files by the authorities referred to in Article 92(4) as a result of information exchange pursuant to that paragraph, shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the alert or alerts concerning the person or object concerned have been deleted from the Schengen Information System.

2. Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period of time for which such data may be held in such files shall be governed by national law.

Article 114

1. Each Contracting Party shall designate a supervisory authority responsible,. in compliance with national law, for carrying out independent supervision of the data

file of the national section of the Schengen Information System and for checking that the processing and utilization of data included in the Schengen Information System are not in violation of the rights of the person concerned. For this purpose the supervisory authority shall have access to the data file of the national section of the Schengen Information System. 2. Any person shall have the right to ask the supervisory authorities to check the data concerning him which are included in the Schengen Information System, and the use which is made of such data. That right shall be governed by the national law of the Contracting Party to which the request is made. If the data have been included by another Contracting Party, the check shall be carried out in close coordination with that Contracting Party's supervisory authority.

Article 115

1. A joint supervisory authority shall be set up, with responsibility for supervising the technical support function of the Schengen Information System. This authority shall consist of two representatives of each national supervisory authority. Each Contracting Party shall have one vote. Supervision shall be carried out in accordance with the provisions of this Convention, of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, and in accordance with the national law of the Contracting Party responsible for the technical support function.

2. As regards the technical support function of the Schengen Information System, the joint supervisory authority shall have the task of checking that the provisions of this Convention are properly implemented. For this purpose it shall have access to the technical support function.

3. The joint supervisory authority shall also be competent to examine any difficulties of application or interpretation which may arise during the operation of the Schengen Information System, to study problems which may arise with the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of the right of access to the system, and to draw up harmonized proposals for the purpose of finding joint solutions to problems.

4. Reports drawn up by the joint supervisory authority shall be forwarded to the authorities to which the national supervisory authorities submit their reports.

Article 116

1. Each Contracting Party shall be responsible, in accordance with its national law, for any injury caused to a person through the use of the national data file of the Schengen Information System. This shall also be the case where the injury was caused by the reporting Contracting Party, where the latter included legally or factually inaccurate data.

2. If the Contracting Party against which an action is brought is not the reporting Contracting Party, the latter shall be required to reimburse, on request, sums paid out as compensation, unless the data were used by the requested Contracting Party in contravention of this Convention.

Article 117

1. With regard to the automatic processing of personal data which are transmitted pursuant to this Title, each Contracting Party shall, not later than when this Convention enters into force, make the national arrangements necessary to achieve a level of protection of personal data at least equal to that resulting from the principles of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, and in compliance with Recommendation R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector.

2. The transmission of personal data provided for in this Title may take place only where the arrangements for the protection of personal data provided for in paragraph 1 have entered into force in the territory of the Contracting Parties concerned by the transmission.

Article 118

1. Each of the Contracting Parties shall undertake, in respect of the national section of the Schengen Information System, to take the measures necessary to:

(a) prevent any unauthorized person from having access to installations used for the processing of personal data (checks at the entrance to installations);

(b) prevent data media from being read, copied, modified or removed by unauthorized persons (control of data media):

(c) prevent the unauthorized entry of data into the file and any unauthorized consultation, modification or deletion of personal data included in the file (control of data entry):

(d) prevent automated data processing systems from being used by unauthorized persons by means of data transmission equipment (control of utilization);

(e) guarantee that, with respect to the use of an automated data processing system, authorized persons have access only to data for which they are responsible (control of access);

(f) guarantee that it is possible to check and establish to which authorities personal data may be transmitted by data transmission equipment (control of transmission):

(g) guarantee that it is possible to check and establish a posteriori what personal data has been introduced into automated data processing systems, when and by whom (control of data introduction);

(h) prevent the unauthorized reading, copying, modification or deletion of personal data during the transmission of data and the transport of data media (control of transport).

2. Each Contracting Party must take special measures to ensure the security of data when it is being transmitted to services located outside the territories of the Contracting Parties. Such measures must be communicated to the joint supervisory authority.

3. Each Contracting Party may designate for the processing of data in its national section of the Schengen Information System only specially qualified persons subject to security checks.

4. The Contracting Party responsible for the technical support function of the Schengen Information System shall take the measures laid down in paragraphs 1 to 3 in respect of the latter.

CHAPTER 4

Apportionment of the costs of the Schengen Information System

Article 119

1. The costs of setting up and using the technical support function referred to in Article 92(3), including the cost of cabling for connecting the national sections of the Schengen Information System to the technical support function, shall be defrayed jointly by the Contracting Parties. Each Contracting Party's share shall be determined on the basis of the rate for each Contracting Party applied to the uniform basis of assessment of value-added tax within the meaning of Article 2(l)(c) of the Decision of the Council of the European Communities of 24 June 1988 on the system of the Communities' own resources.

2. The costs of setting up and using the national section of the Schengen Information System shall be borne by each Contracting Party individually.