Joint Supervisory Authority

Second annual report of the activities:
March 1997 • March 1998
CONTENTS

Preface

Chapter I : Introduction

Chapter II : The Joint Supervisory Authority and its Tasks

Chapter III : Activities of the Joint Supervisory Authority from March 1997 to March 1998

Chapter IV : Joint Supervisory Authority Opinions

Chapter V : Joint Supervisory Authority Action Programme

ANNEXES

1. Background

Joint authorities responsible for applying the Convention
The aim and the architecture of the SIS
The SIRENE Bureaux
Personal data protection

2. Organization chart of the Schengen Working Groups

3. Opinions delivered by the Joint Supervisory Authority

4. The Joint Supervisory Authority's Rules of Procedure

5. List of members of the Joint Supervisory Authority

6. Right of access and communication to individuals of information contained in the Schengen Information System concerning them
PREFACE

The second annual report of the Schengen Joint Supervisory Authority (March 1997 to March 1998) covers a decisive and a crucially important period for police cooperation and the Schengen Information System at European level: the enlargement of the area of free movement to citizens from new member states; the strengthening of the joint security and police information system and Schengen's integration into the European Union.

1997 saw recognition of the autonomy and confirmation of the importance of the Joint Supervisory Authority (JSA), as a body responsible for upholding the rights and freedoms of the individual, in particular vis-à-vis the protection of personal data.

The JSA examined a number of fundamental issues, thus effectively ensuring that the Schengen Information System operates in line with the rules and rights laid down in the Schengen Convention. This is reflected in the JSA's analysis of Italy and Greece's data protection laws, its recommendations and opinions on the security requisites for processing and transmitting personal data, the amount of time this data may be kept, alerts on usurped identities and the transmission of certain categories of data to Interpol.

The JSA's important role was recognized by the Schengen decision-making bodies: it was granted its own budget under a separate budgetary heading, it began to receive on a more regular basis the information it required in order to carry out its duties, and it was asked to deliver opinions on a range of different topics. The successive presidencies (Portugal, Austria and Belgium) have attributed ever increasing importance to the JSA.

In line with our plan of action, during this period the JSA has made significant progress towards achieving greater transparency in the way the system works and in providing information to the public.

The JSA announced its previous annual report at a press conference in Lisbon in April 1997, sent it to the European institutions and Schengen authorities, the national authorities submitted it to their respective parliaments, the conclusions were published in various different editions and can be found on the Internet pages of several data protection authorities.
CHAPTER I: INTRODUCTION

In its first annual report, the Joint Supervisory Authority recalled the stages negotiated by the five States which first signed the Schengen Agreement in 1985, up to the signing of the Convention implementing the Schengen Agreement in 1990 and its subsequent implementation in March 1995. It also described how, during this period, the five signatory countries were joined by ten others, which also wished to participate in this area of free movement of persons.¹

It also outlined the compensatory measures provided for in the Schengen Convention to ensure that the aim of abolishing controls at the internal borders of the Member States, thus creating an area of free movement of persons, could be achieved whilst maintaining within that area at least the same level of security as before. Please find below a brief reminder of those compensatory measures.

The compensatory measures accompanying the abolition of controls at the internal borders provided for in the Convention include harmonization of visa policy, a common policy towards asylum seekers, an improvement in police and judicial cooperation, stronger measures to combat drugs trafficking, harmonization of controls at the external borders of the Schengen territory and the creation of a Schengen Information System (SIS).

The latter links up all the countries already implementing the Schengen Convention and enables its users (police authorities, embassies and consulates etc.) to gain immediate access to the information they require, regardless of which Schengen State originally entered the data.

The system contains information on individuals (those wanted for extradition, non-admissibles, missing persons, persons to be placed under discreet surveillance) and objects (vehicles, arms, documents and banknotes, stolen, missing or forged).

The creation of the SIS was accompanied by the establishment of a Joint Supervisory Authority with responsibility for monitoring the protection of personal data and, in particular, for ensuring compliance with the provisions of the Convention relating to the SIS technical support function (Article 115). The Convention also entrusts the Joint Supervisory Authority, which is made up of two members of the national supervisory authority of each Member State, with an advisory role and with the task of harmonizing legal practice and interpretation at national level.

¹The following states are Members of the JSA: Austria, Belgium, France, Germany, Greece, Italy, Luxembourg, the Netherlands, Portugal and Spain. The five Nordic states (Denmark, Finland, Iceland, Norway and Sweden) participate in the work of the JSA as observers.
CHAPTER II: THE JOINT SUPERVISORY AUTHORITY AND ITS TASKS

In addition to its main responsibility, one which it alone is allowed to discharge (Article 115 (2)) i.e. supervision of the technical support function to the SIS, the JSA has been assigned an advisory function and the task of harmonizing legal practice and interpretation at national level.

The Convention implementing the Schengen Agreement lays down the tasks of the JSA in the following articles:

**ARTICLE 106 (3):**

The JSA delivers an opinion in the event that two Contracting Parties cannot reach agreement with regard to data contained in an alert that has been entered incorrectly or unlawfully. The Contracting Party which did not enter the alert has the duty of submitting the case to the JSA.

**ARTICLE 115 (3):**

The JSA analyses problems relating to implementation or interpretation which may arise in connection with the operation of the SIS; it looks at the problems which may arise with regard to the implementation of independent supervision by the national authorities of the Contracting Parties.

The JSA examines the problems which may result from exercising the right of access to data contained in the system;

At a more general level, it drafts harmonized proposals aimed at resolving existing problems.

**ARTICLE 115 (4):**

The JSA reports to the same bodies as the national supervisory authorities.

**ARTICLE 118 (2):**

The JSA is informed about the special security arrangements made by each Contracting Party for transmitting data to bodies or departments located outside the territories of the Contracting Parties.
CHAPTER III: ACTIVITIES OF THE JSA FROM MARCH 1997 TO MARCH 1998

Between March 1997 and March 1998 the JSA held 10 plenary meetings. All of these were held in Brussels, apart from the JSA annual meeting in Lisbon in April 1997, which was also attended by the Chairman of the Executive Committee. In addition to these plenary meetings, the JSA held five select meetings to draw up 'draft opinions' on specific problems, write its annual report and consider future arrangements for C.SIS inspections. Moreover, on three occasions several of its members met representatives from the French Ministry of the Interior, in its capacity as the body in charge of the C.SIS technical support function. One of these meetings was attended by a Troika of the Schengen Presidencies, inter alia to take stock of the situation regarding the follow-up to the JSA's recommendations after its inspection of the C.SIS.

It should also be borne in mind that since the JSA meeting on 7 March 1997, Sweden, Denmark, Finland, Norway and Iceland have attended JSA meetings as observers pursuant to the decision taken by the Authority in Strasbourg at its meeting of 10 and 11 February 1997.

The following issues have been dealt with in the course of these meetings:

1. **JSA**

   **JSA membership**

   The JSA acknowledged the Greek and Italian personal data protection laws. This is one of the conditions which have to be met before any personal data can be entered in the SIS (Article 117), and is therefore a prerequisite for the Convention to be implemented in the territory of the Contracting States.

   The JSA amended its rules of procedure in order to grant JSA member status to the representatives of the national supervisory authorities of the countries which have acceded to the Schengen Convention, as soon as all the other conditions have been met and the Convention has been brought into force on their territory.

   On the basis of this criterion, at its meeting on 12 December 1997, the JSA decided that representatives from the Italian, Austrian and Greek national supervisory authorities could, henceforth, participate in its meetings as JSA members.
ork. The JSA also believes that the current secretariat, which has been assisting the JSA since the Convention was drafted, is the best placed to lend support.

2. **MATTERS DEALT WITH BY THE JSA**

**JSA OPINIONS**

The JSA has adopted several opinions, listed below in Chapter IV.

**C.SIS INSPECTION**

The definitive version of the confidential technical report on the inspection of the C.SIS carried out in October 1996, which included comments from the French Ministry of the Interior, was adopted. A draft version of this report was sent to the Chairman of the Central Group, whilst the definitive version was sent on 22 April 1997 to the Chairmen of the Executive Committee and the Central Group for onward transmission to the relevant technical groups.

The latter were asked to check to what extent the recommendations on securing the SIS made by the JSA could be acted upon. Almost two years after the inspection, the official Schengen bodies still have not informed the JSA of the action they intend to take further to its recommendations.

**PROVISIONS FOR JSA INSPECTIONS OF THE C.SIS**

The abovementioned draft conditions governing future inspections of the C.SIS were examined during the year. At the meeting of 12 December 1997, the majority of the members of the Joint Supervisory Authority agreed that the draft conditions, which had been drawn up over the course of several meetings between the representatives of the French Ministry of the Interior and the JSA, ignored the independent status of their Authority.

As a result, it was decided that a select group would be appointed to deal with this delicate matter and to come up with a new document taking account of the security requirements set by the French Ministry of the Interior and also the need for the JSA to carry out their controls independently.

A new version was drafted by a select group of JSA members on 2 February 1998, to be approved at the plenary meeting of 6 March 1998. It will act as a new basis for discussions with those concerned.
The press conference was attended by various Portuguese journalists from television, radio, major daily newspapers and Portuguese news agencies, as well as several foreign journalists, in particular from the EFE Agency (Spain) and Reuters (GB). In addition, further publicity was given to the JSA meeting and the presentation of the annual report in other periodicals.

The most pertinent issues for the media were the definition of the duties of the JSA, its role within Schengen, the functioning of the SIS, the type of data it contained and means of access, as well as general information on the Schengen Convention.

The report was distributed by the national supervisory authorities using the same channels as for their national reports, as well as by Internet in some cases. In some countries press conferences were held to present the document and to heighten public awareness of the JSA.

TRANSPARENCY IS FOR THE PUBLIC

In a move aimed at fulfilling its obligation to inform the public, the JSA decided to publish a leaflet explaining the rights of individuals who were the subject of information entered in the SIS.

On 12 December 1997, the Joint Supervisory Authority adopted the definitive version of the text outlining the individual’s right of access to SIS information which concerns them and selected one of the designs submitted by one of the advertising agencies it had consulted.

This text, which is annexed hereto, comes in the form of an information leaflet and will be distributed to the authorized crossing points at Schengen’s external borders. Posters will be put up to inform the public that these leaflets are available.

The success of this initiative will hinge on how well the documents are distributed. The JSA is therefore counting on the support of the national supervisory authorities, the Schengen bodies and the competent national authorities.

INFORMATION FOR THE JSA

In April 1997, at the request of the Joint Supervisory Authority, the Central Group asked the C.SIS and Management Unit to make their monthly reports available to the JSA. The JSA felt it necessary to have these documents to ensure that the rules governing personal data protection were being upheld.
CHAPTER IV: JOINT SUPERVISORY AUTHORITY OPINIONS

On examination by the Joint Supervisory Authority, it emerged that several of the opinions under scrutiny required additional information. This explains why some of the opinions mentioned below already appeared in the first annual report. Furthermore, the first two opinions included here, approved in March 1997, can also be found in the previous report. The opinions are briefly summarized below and reproduced in their entirety in the annex to this report.

1. **OPINION OF 7 MARCH 1997 ON THE “TRAFFICKING OF STOLEN VEHICLES” PILOT PROJECT - WORKING GROUP I ON POLICE AND SECURITY** (SCH/AUT-CONT (97) 22 REV)

On 10 February 1997, the Central Group sent the JSA a request from Working Group I on Police and Security for its opinion on the participation of countries not yet integrated into the SIS in a pilot project on stolen vehicles.

Having noted that this project tended to enable countries not yet integrated into the SIS to consult the system via their liaison officers, the JSA asked for additional information on the nature of the information exchanged and the means used to transmit it.

This information was communicated to the JSA, which delivered an opinion on 7 March 1997, in which it pointed out that:

- information on the make, type, colour and technical features of a vehicle is not in itself regarded as data of a personal nature if there is no link between such information and the registration number or the owner or the driver of the vehicle;

- the exchange of police information from national files between Contracting Parties integrated into the SIS and other States where the Convention has not yet been implemented, via channels for bilateral and multilateral cooperation, is subject to national data protection legislation and under the control of the national supervisory authorities,

However, the JSA took the view that directly or indirectly personalized data recorded in the SIS should not be accessible and could not be consulted directly by the authorities of Contracting Parties on whose territory the Convention had not
yet been implemented, in accordance with Articles 101 and 126 (1) of the Convention.

This opinion was communicated to Working Group I, which took it into account in implementing its project. Other pilot projects, such as the pilot project on drug routes currently in preparation, should also bear it in mind.


On 10 February 1997, the Central Group sent the JSA a request from Working Group III on Judicial Cooperation for its opinion on a proposal for a draft Cooperation Agreement on road traffic offences.

The text provides for access to information and data in the Contracting Parties' vehicle registration files and for a system of direct notification and cooperation, as well as for the actual enforcement by each Contracting State of decisions from an authority of another Contracting Party, without prejudice to specific cases which restrict or rule out the enforcement of a fine.

This project is based on the Joint Declaration of the Ministers and Secretaries of State of 19 June 1990, in which the Contracting Parties undertake to initiate or continue discussions in various fields, including proceedings for road traffic offences and the reciprocal enforcement of fines.

While the Agreement constitutes a separate international legal instrument, it also complements the Schengen Convention, and reference is made to Title VI of the latter on the rules governing data protection when exchanging information not recorded in the SIS.

Having examined the provisions on data protection laid down in the draft Cooperation Agreement, the JSA delivered an opinion on 27 March 1997 requesting that the following principles be incorporated or clarified:

- the right of every person to have data containing factual or legal errors corrected or deleted.
- the principle of cooperation between the national supervisory authorities listed
under Article 128 (1) with a view to guaranteeing the rights of access, correction or deletion;

- the JSA's powers to issue an opinion on the common aspects of protection of personal data resulting from the Agreement's implementation.

This opinion was sent to Working Group III which consequently adapted its draft opinion.

3. **Opinion 97/1 of 22 May 1997 on Copying SIS Data** (SCH/AUT-CONT (97) 38 REV)

Article 102 (2) stipulates that data recorded in the SIS may only be copied for technical purposes, provided that such copying is necessary so that the authorities referred to in Article 101 can carry out a direct search.

At the request of the Belgian Committee responsible for issues relating to personal privacy, the JSA initiated a discussion in regard to this Article on how to interpret the phrases "copying for technical purposes" and "direct search", particularly with reference to the automated search procedure mentioned in Article 92.

The JSA also started assessing the consequences of CD-ROM duplication of an entire N.SIS or part thereof for the purpose of searches by consular or diplomatic representations.

The review of the conditions for implementing Article 102 (2) raised questions related to the updating of duplicated information and to the level of security of transmission to offices located outside the territories of the Contracting Parties.

Consequently, the JSA proposed a co-ordinated solution which is compatible with the rules governing data protection laid down by the Convention.

In Opinion 97/1, it pointed out that whatever means were used by the diplomatic missions and consular posts of certain Schengen States abroad to search SIS data pursuant to Article 96 of the Schengen Convention, the following rules had to be observed:

- The methods and means of duplication should guarantee that data is identical, in real time, to data processed at the C.SIS.
• At least the level of protection required in Article 118 (1) of the Schengen Convention and especially its subparagraphs b), d) and f) should be guaranteed and the provisions of Article 118 (3) of the Schengen Convention should be observed.

• The programme on which they are based should enable data to be recorded in accordance with the provisions of Article 103 of the Schengen Convention:

These records should be returned to the Schengen State every six months and made available to the national supervisory authority provided for under Article 114 of the Schengen Convention, by the body with central responsibility for the national section of the SIS provided for under Article 108 (1) of the Schengen Convention.

In the event that duplication aids are used which entail the risk that the data will not be identical, the JSA urged that the Contracting Party assumes its responsibility, as provided for in Articles 92 (2) and 116 of the Convention, as follows:

- where an alert exists for an individual in the duplicated aid used, the Contracting Party shall carry out a real-time check (network, telephone, Fax) to confirm the accuracy of this information;

- where no alert exists for an individual in the duplicated aid used, the Contracting Party shall accept responsibility in the event that an alert is issued for the same individual in the space of time between the duplication of the data and real time. This responsibility may be relinquished only if there is proof of a real-time check at the time of the visa application.

On examining this matter, the JSA found that, contrary to the provisions of Article 118 (2), it had not been advised of the specific measures taken to ensure data security in such cases.

On 6 December 1996, therefore, the JSA asked the Central Group to provide it with details of the measures taken by the Schengen States to comply with Article 118 (2) of the Convention.

At the time of writing, the JSA is still awaiting this information, which it will use to check whether the measures being implemented in the States comply with its interpretation of the Convention.
4. **Opinion 98/1 of 3 February 1998 on Archiving Documents After Alerts Have Been Deleted** (SCH/AUT-CONT (97) 55 REV 2).

The JSA's attention was also drawn to difficulties arising in connection with Article 102 (1) from the retention of documents on alerts after their deletion.

In fact, Article 102 (1) prohibits the Contracting Parties from using the data stipulated in Articles 95 - 100 for purposes other than those laid down for each type of alert referred to in those articles.

However, the national police departments in certain Contracting Parties keep documents relating to alerts even after alerts issued pursuant to Article 95 (1) of the Convention have been deleted and use them to compile criminal files.

For this purpose the police authorities invoke provisions in national data protection law (see Point 2.1.3. b of the SIRENE Manual) and the provisions of Title VI of the Convention.

The JSA considered this matter to be extremely important in relation to the purpose for which alerts were used. In its opinion of 3 February 1998, the Joint Supervisory Authority pointed to the fundamental principles and rights laid down in the Convention with regard to data protection, and in particular to the following:

a. data may be supplied and used solely for the purposes laid down for the alert itself (Article 102(1) and Article 94(1) of the Convention). A derogation from this general principle may only be made if it is necessary in order to avert an imminent serious threat to public order and safety or for compelling reasons of national security or for the purpose of preventing the commission of a serious offence (Article 102(3)).

b. Any use of data which does not comply with Article 102 (1 to 4) shall be regarded as misuse (Article 102(5)).

c. Pursuant to Article 112 of the Convention, personal data saved in the Schengen Information System for the purpose of locating persons shall be stored no longer than is necessary for the intended purpose.

d. These basic principles shall apply by way of a complementary interpretation of legally binding texts to all types of data processing relating either directly or indirectly to alerts in the Schengen Information System.
The Joint Supervisory Authority therefore believes the following measures should be taken:

a. After an alert issued for the purpose of locating an individual has been deleted, every Contracting Party to the Schengen Convention shall, pursuant to Article 112 of the Convention, destroy all its accompanying documents immediately.

b. The Schengen bodies shall revise the SIRENE Manual with a view to deleting the provisions under 2.1.3 b) which contravene the Schengen Convention.

5. **OPINION 98/2 ON ENTERING AN ALERT IN THE SCHENGEN INFORMATION SYSTEM ON INDIVIDUALS WHOSE IDENTITY HAS BEEN USURPED**
(SCH/AUT-CONT (97) 42 REV 2)

In cases of impersonation, alerts for persons who have usurped someone else's identity are entered in the SIS in certain countries under the name of the person who has been impersonated.

In other words, the system contains an alert with an identity which corresponds neither *de facio* nor *de jure* to the real identity of the wanted person, and the identity of the person who has been impersonated is entered in the SIS without this person receiving any prior notification.

Some States are in favour of a procedure whereby personal data relating to persons who have been impersonated should be deleted immediately, whereas other States argue that the alert containing the usurped identity should be retained even if the person whose identity was incorrectly entered in the SIS requests that this data be deleted. The argument put forward by those in favour of maintaining the alert is that the impersonator must be found.

The JSA has examined the problems encountered as a result of the misuse of aliases by individuals who are the subject of an alert in the SIS in the light of the principles governing data protection laid down in the Schengen Convention. It has reiterated the following fundamental rights and principles with regard to data protection:

a. The data may be supplied and used solely for the purposes intended for each alert (Articles 102 (1) and Article 94 (1)); any derogation from this rule shall be exceptional and justified by the need to prevent an imminent serious threat or a serious offence (Article 102 (3)).
b. Any use of data which does not comply with paragraphs 1 to 4 shall be regarded as misuse (Article 102 (5)).

c. The right of an individual who finds that data relating to their person is factually or legally inaccurate to have this information corrected or deleted (Article 110 (1)).

d. The right of an individual to bring an action before the courts or the authority competent under national law to correct or delete data in an alert concerning them (Article 111 (1)).

e. The right of an individual to ask the supervisory authorities to check data in an alert concerning them (Article 114 (2)).

The JSA, taking due and balanced account of the rights as laid down in the Schengen Convention of the person whose identity has been usurped and the need to detect the impersonator hereby delivers the following opinion:

1. Entry of data in the SIS on individuals whose identity has been usurped shall be governed by national law, unless more stringent conditions are laid down in the Schengen Convention (Article 104 (1)).

2. The Contracting Party issuing the alert shall guarantee that data is entered solely for the specified purposes and that it is up-to-date and correct (Article 102 (1), Article 106 (1), Article 110, and the provisions relating to data protection laid down in the Council of Europe Convention (No. 108), inter alia those contained in Article 5, which are binding on the Schengen States).

3. The Contracting Party issuing the alert shall guarantee the right to correction or deletion of the data stored, in accordance with the procedure laid down in Article 106 of the Schengen Convention:

4. The question as to whether an alert on an individual whose identity has been usurped should be kept in the SIS should be evaluated in accordance with the proportionality principle, with consideration given on the one hand to the rights of the person whose identity has been usurped and on the other to the need to detect the impersonator.

5. In the interim period until the SIS II is brought into service, an appropriate, and if possible, joint solution should be sought and adopted so as to indicate that the alert is on a usurped identity. The JSA would be willing to cooperate to help find a solution of this nature.
6. **Opinion 98/3 on the possibility of linking the Schengen Information System and the “Interpol ASF-stolen vehicles” project**

This proposal, outlined in a note from the SIS Steering Committee, involves transmitting SIS data in respect of individuals and stolen vehicles, and at a latter stage other categories of data, to an Interpol database.

The JSA restated many of the Schengen Convention's principles, gave its opinion on Schengen’s “stolen vehicles” pilot project and, focusing solely on the protection of personal data, issued the following opinion:

1. Information and personal data contained in the Schengen Information System cannot be transmitted to Interpol in connection with the ASF - stolen vehicles project without breaching the provisions of the Convention, and in particular Articles 101, 102, 118 and 126.

2. Information on the make, type, colour and technical features of the vehicle is not personal data as such within the meaning of the Schengen Convention.

3. The transmission of information to Interpol as part of the ASF - stolen vehicles project does not breach the provisions on the protection of personal data contained in the Convention, insofar as the data cannot be linked to the identity of the person connected with the vehicle.

4. Police exchanges of information on stolen vehicles, taken from national files, are governed by the relevant national legislation, and more specifically legislation on data protection.

7. **Opinion 98/4 on the interpretation of Article 103: checking whether SIS searches are acceptable or not**

The JSA’s attention was drawn to the difficulties encountered in implementing Article 103 of the Convention, in relation to the recording of every tenth transmission of personal data in the national section of the Schengen Information System by the authority responsible for the data file.

Taking into account that the Schengen Information System (SIS) is an automated
search system which requires effective protection from unauthorized access by third persons, the JSA concluded that logging a representative average number of times the system is consulted constitutes an appropriate means of preventing unauthorized access.

The JSA has conducted a study of the various technical solutions adopted by each Contracting State to comply with Article 103.

It found that the Contracting Parties interpret differently the requirement laid down in the Convention i.e. that every tenth transmission of personal data be recorded in the national section of the Schengen Information System by the authority responsible for the data file for the purpose of checking whether the search is acceptable or not (Article 103).

The JSA issued an opinion on the interpretation of this article with a view to harmonizing the Contracting Parties' approach.

The Joint Supervisory Authority considered that recording as laid down in Article 103 of the Schengen Convention should comply with the following minimum requirements:

1. The log must be sufficiently representative of all consultations, regardless of whether the outcome was a hit or a negative response. The minimum requirement of 10 per cent can also be met by recording at regular intervals.

2. The most important elements for appropriate logging are as follows:
   a. biographical data transmitted on the person on whom the search is run.
   b. identification of the terminal or the authority which carried out the search, ensuring that all the necessary measures are taken to enable the user to be identified,
   c. place, date and time of the search;
   d. grounds for consultation, e.g. the legal basis for the alert.

3. In addition, the following are also desirable for checking the admissibility of data searches in individual cases: the reference number or police day book number, if this exists, used for locating the relevant file.

The data shall be used solely for the purposes laid down in Article 103.
The recorded data shall be deleted within six months.

The JSA insisted that the requirement laid down in Article 103 of the Convention be taken into account in accordance with its opinion.
CHAPTER V: ACTION PROGRAMME

The action programme put forward by the Chairman of the JSA for the first half of 1998 was adopted on 3 February 1998.

This programme aims to strengthen the JSA's role within Schengen, outlines its priority measures aiming to guarantee data protection and recommends greater cooperation between the Schengen bodies.

The JSA will continue to act in an advisory capacity and will pursue its task of harmonizing national legal practices and legal interpretations by continuing to issue opinions. It will see to it that the opinions it has adopted have been adequately publicized by the Central Group - failing this, it will reach an agreement on publication of its opinions.

Special attention will be paid to the measures taken by the Schengen decision-making bodies in response to JSA opinions and recommendations, in particular where C.SIS security is concerned. Indeed, although both Schengen Presidencies in 1997 instructed the technical groups to examine the JSA's recommendations, the JSA feels that this issue has not yet been accorded the priority it deserves.

The JSA would like the Schengen bodies to inform it very quickly of the action they intend to take further to its recommendations. This applies in particular to the JSA's request for a special user account to facilitate checks.

While the proposed user account would not provide the facility to make changes, it would give the JSA direct access to the operating system and databases, thus making it easier to carry out C.SIS checks.

Security in the Sirene Bureaux will be subject to special inspections in all countries in the future, followed by a final report.

The JSA will see to it that the leaflet on the individual's right of access to SIS data which concerns them is distributed to the authorized crossing points at the external borders of the Schengen area.

The JSA will strengthen its ties with EU representatives, pending the integration of the Schengen acquis into the Union, in particular by participating in the definition of its acquis. This issue will be crucial for the development of European police systems.
At its press conference in Brussels on 28 April 1998, it will present its annual report to the general public and to the press.

On 30 June 1998, it will hold a colloquium in Lisbon on the topic of individual rights vis-à-vis police information systems, based on the Schengen model.
DECLARATION OF THE JSA OBSERVER STATES

"Having observer status in the JSA, the Nordic countries share the concerns of the full members as expressed in the annual report. They also share the main viewpoints expressed in the opinions referred. Among other things, it is of greatest importance that the advice and opinions given is observed and respected by the central as well as the national bodies in the Schengen system.

The presence of the Nordic national data and privacy protection commissions in the JSA is of utmost importance in the efforts aiming at ensuring common, public acceptance and support of the important work done in accordance with the Schengen Convention. The Nordic observers are of the opinion that the JSA may need to have its economic resources strengthened in the future. They see an immediate need to further strengthen the administrative capacity of the secretariat but will also not exclude the need for more formal authority."
BACKGROUND
I. **JOINT BODIES RESPONSIBLE FOR IMPLEMENTING THE CONVENTION**

The Contracting Parties created the following two bodies for the purpose of implementing the Convention:

- The Executive Committee, consisting of the ministers responsible for applying the Convention in the respective Schengen States. The task of the Committee is to ensure that the Convention is correctly implemented. It also possesses special powers (Article 131).

- The Joint Supervisory Authority (JSA), which consists of two representatives from the national control authority in each of the respective Schengen States. It has the task of ensuring that the provisions of the Convention relating to the technical support function of the SIS (Article 115) are correctly applied. It also possesses more general powers in the area of data protection.

In addition to these two bodies, there is the Central Group, which oversees a Steering Committee and a number of working groups, some of which were set up directly pursuant to the Convention.

Administrative support for the Schengen committees and groups is provided by the General Secretariat of the Benelux Economic Union, which is based in Brussels.

An organogram is annexed to this report.

II. **OBJECTIVES AND ARCHITECTURE OF THE SCHENGEN INFORMATION SYSTEM**

Title VI of the Schengen Convention is devoted entirely to the Schengen Information System (SIS).

Article 93 of the Convention stipulates that the purpose of the SIS is to use the information provided via the system to safeguard public order and security, including national security, and ensure that the provisions contained in the Convention with regard to the movement of persons are applied.
Article 94 contains a detailed list of categories of data that can be stored in the system. The purposes for which alerts may be entered are given in Articles 95 to 100.

The above categories relate to persons, objects and vehicles.

- Data on persons may include marital status, possible aliases and any specific and objective physical characteristics not subject to change; data may also indicate whether a person is armed or violent and what steps are to be taken if the person is discovered.

"Sensitive" information, e.g. concerning racial origin and political, religious or other beliefs, and information concerning a person's health and sexual activities may not be entered.

An alert for a person may be entered in the SIS for the following reasons:

a. Regardless of nationality:
   - arrest for the purpose of extradition (Article 95)
   - to determine the whereabouts of a missing person, of minors or of persons whose detention has been ordered by the competent authorities (Article 7); arrest for the purpose of appearing in court, either as a suspect or a witness; at the request of the judicial authorities in connection with a criminal investigation or for the purpose of serving a custodial sentence (Article 98);
   - discreet surveillance and specific checks, conducted for the purpose of prosecution in connection with a criminal offence, averting a threat to public safety or national security (Article 99).

b. In the case of aliens, i.e. persons who are not nationals of any of the Member States of the European Communities (as defined in Article 1, paragraph 6):
   - refusal of entry to the Schengen area pursuant to a decision taken by the competent administrative or judicial authority subject to national laws, a decision based on the danger posed to national security and public order or a decision based on the fact that the alien concerned has contravened national provisions governing entry and residence (Article 96).
With regard to objects, the only data that may be entered, apart from the name of the owner, is that relating to vehicles, firearms, documents and banknotes which have been stolen, misappropriated or lost and which are sought for the purpose of confiscation or for use as evidence in criminal proceedings (Article 100).

Likewise, data on vehicles may include information on vehicles that are sought for the purpose of discreet surveillance or specific checks (Article 99, see above). This category can also include information relating to the driver and the passengers of the vehicle concerned.

Access to Information

Articles 92 and 101 of the Convention state that authorities designated by the Contracting Parties are entitled, either by means of an automated search procedure or otherwise, to have access to:

- all the data stored in the SIS: for the purpose of border checks and police and customs checks carried out in the country in accordance with national law;

- only the category of alerts entered for the purpose of refusing entry: for the purpose of issuing visas, residence permits and the registration of aliens for the purpose of applying the provisions of this Convention on the movement of persons.

The list of authorities authorised to search the SIS directly should be sent to the Executive Committee (Article 101 (4)).

Architecture of the Schengen Information System

Although several articles in Title IV lay down that certain technical measures should be observed, the general description of the system is given in Article 92.

The Schengen Information System (SIS) consists of one national section (N.SIS) for each of the Contracting Parties, and a technical support function (C.SIS), set and maintained jointly. Responsibility for the system rests with the French Republic.

The technical support function, based in Strasbourg, serves to ensure that all the national systems are essentially identical. The C.SIS therefore has a database which ensures that national databases are identical by providing information on line.
Data is transmitted in accordance with protocols and procedures established jointly by the Contracting Parties for the technical support function.

Article 118.4 stipulates that the safety measures taken for the technical support function must be identical to those that have to be taken by the various national SIS’s (Article 118 (1-3)).

III. *THE SIRENE BUREAUX*

The SIRENE bureaux (Supplementary Information Request at the National Entry) were set by the Contracting Parties. They are not expressly provided for in the Convention.

The national SIRENE bureaux are responsible for exchanging additional information based on the SIS. They also operate as intermediaries when the States hold consultations to determine what action to take when an alert is implemented.

Their tasks and activities are described in detail in a common manual known as the “SIRENE Manual”. The main task of the SIRENE bureaux is to consult before an alert is entered, exchange information, check to ensure that multiple alerts have not been entered and set priorities.

IV. *PROTECTION OF PERSONAL DATA*

1. **NATIONAL LAW AND A NATIONAL SUPERVISORY AUTHORITY : PREREQUISITES FOR IMPLEMENTING THE CONVENTION**

The Schengen States have laid down a number of prerequisites for the implementation of the Convention on their respective territories. The Final Act lays down that fulfilment of these prerequisites is compulsory.

One of these prerequisites concerns the mandatory establishment of a national supervisory authority (Articles 114 and 128) and introduction of personal data protection legislation before any personal data can be transmitted.

With regard to the automatic or non-automatic processing of data provided in accordance with the Convention, the latter contains the following provisions:

*a. for the automatic processing of data provided for the purpose of implemen-
As regards the automatic processing of personal data which is transmitted pursuant to this Title, each Contracting Party shall, no later than the date of entry into force of this Convention, take the requisite steps at national level to ensure a degree of protection of personal data at least equal to that resulting from the principles laid down in 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 accordance 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.

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.

b. for the automatic processing of other data transmitted pursuant to the Convention, apart from data relating to applications for asylum:

This article lays down that at the time of the Convention's entry into force, the level of protection of personal data should be at least equal to the level resulting from the principles laid down in the Convention of the Council of Europe of 28 January 1981 and that data must not be transmitted unless this level of protection actually exists in the territory of the Contracting Parties involved in the transmission.

With regard to the transmission of data relating solely to police cooperation, the Contracting Parties should create a level of protection that is in keeping with the principles of the abovementioned Recommendation R (87) 15 of the Committee of Ministers of the Council of 17 September 1987.

c. With regard to the transmission pursuant to the Convention of data taken from or entered in a non-automated data file, apart from data relating to applications for asylum, the SIS or mutual assistance in criminal matters:
**ARTICLE 127**

Application of the provisions of Article 126 and, where the transmission of data for the purpose of police cooperation is concerned, a level of protection that complies with the principles contained in the above Recommendation R (87).

d. Lastly, with regard to the transmission of data not stored in non-automated data files, the specific provisions on protection contained in Article 126 (3) apply, with one exception. The national supervisory authority shall if necessary supervise transmission (Article 128, paragraph 2).

**2. THE SCOPE OF THE SCHENGEN CONVENTION AND THE SCOPE OF NATIONAL LAW**

With regard to the protection of personal data, the Schengen Convention creates a complex distinction between the scope of the provisions of the Convention and the scope of the national law of the Contracting Parties.

**THE RIGHTS OF THE INDIVIDUAL WITH REGARD TO THE SIS**

The general rule here is that where the Convention contains no specific provisions, the national law of the Contracting Parties applies.

The Convention specifies the rights of the individual and any limitations placed upon them. These rights are exercised subject to the aforementioned provisions and in accordance with the national law of the Contracting Parties.

a. **Right of access to information and communication of information** (article 109)

Every person has the right of access to information stored in the SIS which relates to him. He or she should submit a request for this purpose to any of the Contracting Party's competent authorities.

Information concerning the person submitting a request may be communicated to him, national law permitting. In accordance with the principle of data ownership, the State which has received the request and which is not responsible for entering the data in the SIS must first give the Contracting Party which issued the alert the opportunity to give its opinion.

Communication of information may be refused if there is possibility that it may jeopardise the fulfilment of the task specified in the alert or if it is essential in
order to protect the rights and freedoms of third parties. It will in any event be refused if the person concerned is the subject of an alert issued for the purpose of discreet surveillance.

b. Right to have information corrected (Article 110)

Anyone has the right to have inaccurate information concerning him or her corrected or deleted. In practice, communication of the data stored in the system facilitates the exercise of this right.

c. The right to bring an action for the purpose of correction, deletion, communication of information or to obtain compensation (Article 111).

Any person is entitled to exercise his or her rights before the competent court or authority in the territory of any of the Contracting Parties. Final decisions in such matters are enforced by the Contracting Party concerned.

d. Right to request that the data be checked (Article 114(2))

Any person has the right to request the supervisory authorities to check the data stored in the SIS which relates to him, as well as the use made of it. If the data has been entered by another Contracting Party, the check shall be carried out in close consultation with the supervisory authorities of the Contracting Party which has entered the alert.

Although an exhaustive list of the requests submitted to the Schengen States for the purpose of exercising the abovementioned rights has not yet been drawn up, the information available shows that the number of requests per State in the past two years is between one and forty.

SUPERVISION OF THE SCHENGEN INFORMATION SYSTEM

The principles on data protection which apply without prejudice to the national law of the Contracting Parties to the processing of data stored in the SIS are laid down in Article 104 of the Convention. For the purpose of supervising compliance, the Convention provides for the Joint Supervisory Authority and the national supervisory authorities to share responsibility.

The principles contained in the Convention are as follows:

a. The principle that information should be entered in the SIS, except in certain cases which are listed in detail, for a particular purpose and used only for that
purpose: extradition, refusal of entry, missing persons, witnesses, persons summoned or convicted, stolen objects, persons or vehicles subject to discreet surveillance or specific checks (Articles 94 to 100, see above).

b. Ban on processing sensitive data and an exhaustive list of data that has been entered (Article 94, see above).

c. Definition of the persons or bodies with access to the data: access restricted to national authorities competent in certain areas and only in so far as such access is necessary to enable them to perform their tasks (Article 101, see above).

d. Ban on copying alerts entered by other Contracting Parties in a national database and restriction on duplication for technical purposes (Article 102).

e. Obligation to record every tenth transmission of personal data for the purpose of checking whether the search is acceptable (article 103).

f. Laying down a fixed period of time for keeping data (Articles 112 and 113).

g. Obligation to preserve deleted data for one year in technical support function for the purpose of retrospective accuracy checks and to determine whether it was lawfully entered (Article 113 (2)).

With regard to checks on the system, the Convention lays down that each of the Contracting Parties must appoint a national authority to perform the task of supervising the national section of the Schengen Information System (N.SIS) independently and in accordance with national law (Article 114).

These authorities are responsible for examining whether the data protection provisions contained in the Convention and any provisions applicable under national law are being complied with.

Supervision of the technical support function (C.SIS), on the other hand, is allocated to the Joint Supervisory Authority, which must perform its tasks in accordance with the Schengen Convention, the Convention of the Council of Europe for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Recommendation of the Council of Europe regulating the use of personal data by the police, and pursuant to French law.
Title VI (Articles 126 et seq.) of the Convention, entitled "Protection of Personal Data", focuses on the rules that apply to information exchanged in the context of implementing the Convention but not based on data entered in the SIS. (cf. point 2.1, b and c).

The principles laid down (use of the data solely for the intended purpose, restrictions on the d rights has not yet been drawn up. the information available shows that the number of requests per State in the past two years is between one and forty.

Supervision of compliance with the rules contained in the Convention is the task of the national supervisory authorities.

The JSA plays a complementary role: it may issue an opinion on the problems arising from the application and interpretation of these rules.
OPINION ON THE “ROUTES USED FOR THE TRAFFICKING OF STOLEN VEHICLES” PILOT PROJECT

The JSA was asked to comment on a pilot project on the routes used for the trafficking of stolen vehicles. The question was whether countries which are not linked up to the Schengen Information System can have access to data on stolen vehicles contained in the SIS. The request for an opinion was not accompanied by information on the project: on the participants, the international and national coordination system, the conditions for access to information and its use and future analysis.

In the meantime, however, we have managed to glean the following information:

The pilot project is aimed at improving European police cooperation in combating the trafficking of stolen vehicles, and in particular by identifying international trafficking networks, routes and means employed.

The coordinated joint operations at predetermined border points and areas, will involve police forces which are responsible, in the different states, for border controls and traffic, customs, fiscal and criminal controls.

The following States are involved in the project:

The Contracting Parties to the Schengen Convention who enter alerts and who have access to the Schengen Information System (Germany, Belgium, Spain, France, Luxembourg, the Netherlands and Portugal).

The Contracting Parties to the Schengen Convention or the Cooperation Agreements with the Schengen States, who, for one reason or another, have not yet begun implementing the Convention and who therefore do not enter alerts into the system nor do they have access to the SIS (Austria, Greece, Italy, Denmark, Finland, Norway and Sweden).
This leads us to the question of personal data protection.

The JSA

Whereas,

a. access to data contained in the Schengen Information System, and the right to search such data directly shall be reserved exclusively to the competent authorities, in accordance with a list sent to the Executive Committee, which defines the type of alerts to which each authority can have access, (the right to access and consult a specific category of alert depends on the national powers of each authority - Article 101 (1) and (3) of the Convention);

b. users may only use the data for the purposes laid down for each type of alert (purpose behind use - Article 102 (1) of the Convention);

c. national law shall apply to data entered in the national section of the SIS, without prejudice to the application of more specific provisions of the Convention (Article 104 (1));

d. personal data for which the Convention provides may not be transmitted until the Contracting Parties are able to achieve a level of protection of personal data at least equal to that provided for in the Council of Europe Convention No 108 of 28 January 1981 (Article 126 (1) and (2) of the Convention);

e. information on the make, type, colour and technical features of a vehicle is not personal data as such, as this kind of information is not directly linked to the registration number, owner or driver of the vehicle in question (which means that it would be possible to match a vehicle to its manufacturer, without knowing the registered owner);

f. it is possible at a national level for each state involved to allow the police authorities of another State, by means of bilateral or international police cooperation instruments, to have access to the national databases on stolen vehicles, insofar as the national legislation on data protection does not prevent such access;

g. information to the competent authorities of each of the countries participating in the project and information from the country which entered the alert, as long as no other information is divulged, does not breach the provisions on the protection of personal data contained in the Convention;
h. Police exchanges of information on stolen vehicles, taken from national files, between the Contracting Parties linked up to the SIS and the other countries, where the Schengen Convention has not yet been implemented, are governed by national legislation on data protection, and controlled by the national authorities.

has agreed the following:

**OPINION**

1. Information and personal data contained in the Schengen Information System cannot be accessed, nor can it be directly consulted by the authorities of the Contracting Parties which are not yet applying the Convention, in accordance with Articles 101 and 126 (1) and (2) of the Convention.

2. Information on the make, type, colour and technical features of the vehicle is not personal data as such according to the Schengen Convention.

3. Information to the competent authorities of each of the countries participating in the project and information on the country which entered the alert, as long as no other information is divulged, does not breach the provisions on the protection of personal data contained in the Convention.

4. Police exchanges of information on stolen vehicles, taken from national files, are governed by national legislation on data protection, where possible, and insofar as such legislation does not prevent such exchanges.
The Central Group has requested the opinion of the JSA on the cooperation agreement on processing road traffic offences (Doc. SCH/III (96) 25 rev 4).

This Agreement provides that:

1. In the framework of cooperation between the Contracting Parties on processing road traffic offences and their respective enforcement, by communicating a vehicle registration number through their national vehicle registration authorities, States may access information from the national vehicle registration authorities of the other States concerning the type and make of the vehicle as well as the identity (name and address) of the person registered for the vehicle in question when the road traffic offence was committed.

2. The information shall be directly sent to the competent authorities of the requesting State, along with the name and address of the requested authority.

3. Persons suspected of having committed a road traffic offence shall be directly notified by the requesting authority, and shall be sent any extra information enabling the accused person or body to respond to, or contest, the charge.

4. Mutual assistance between the authorities with a view to obtaining a response from the accused party.

5. A system aiming to ensure that the amount of financial penalties is in keeping with the law of the State where the penalty is enforced.

6. The overall competence of the Schengen Executive Committee for overseeing the application of the Agreement.

7. The application of the transmission of personal data under Articles 126-128 of
the Schengen Convention

Following a closer analysis of the area involving protection of personal data, the JSA considers that:

a. The Agreement on processing road traffic offences focuses on two essential areas: access to information and data on vehicle registration in another State, which is a Contracting Party to the Convention; the data may be used solely for the purpose for which it was transmitted and within the competence of the respective national authorities. A system which enables the direct notification and cooperation and enables the authority of a Contracting Party to enforce a decision of an authority of another State, in specific conditions which include the maximum time limits for enforcing a financial penalty or its non-application (when national legislation does not regulate the offence)

b. The data may only be transmitted to countries, i.e. Contracting Parties, which have an autonomous national supervisory authority and which have national provisions on the protection of data and which provide a level of protection of personal data at least equal to that laid down in the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data (as a result of the application of Article 126 (1) and (2) and Article 126 and 128 (1) of the Convention).

c. The personal data shall be limited to the name and address of the vehicle owner and person suspected of having committed the offence.

d. Articles 126 and 128 of the Convention shall apply to the transmission and use of data, which means that data may be used solely for the purposes for which it was transmitted - i.e. the identification and processing of an offence and the enforcement of a financial penalty (principle of purpose). In the same way, the data transmitted cannot not be interconnected on national information systems on road offences.

e. The person in respect of whom the data is transmitted shall be guaranteed the right to know and be informed of where the data was transmitted, and prior notification of the enforcement of the financial penalty shall be guaranteed so that accused parties may respond and defend their case, including the possibility to contest decisions due to mistakes of fact or mistakes of law (Articles 4 and 6 of this Draft).

In the view of the JSA, the following principles still require inclusion or
explanation, on the basis of the rules outlined overleaf:

1. Everyone shall have the right to require the correction or the deletion of data that concerns them, when these are due to mistakes of fact or mistakes of law.

2. The cooperation between the national supervisory authorities, referred to in Article 28 (1), setting out to guarantee rights of access, correction and deletion.

3. The powers of the ACC to deliver its opinion on areas of common interest concerning the protection of personal data, which is a result of the application of this Agreement, a principle that should be mentioned in Article 16 of the Cooperation Agreement.
Joint Supervisory Authority

Brussels, 26 May 1997
SCH/Aut-cont (97) 38 rev
Translation: Orig. FR

OPINION No. 01/97 OF 22 MAY 1997 ON THE DUPLICATION OF CERTAIN SIS ALERTS

Subject: Use of technical duplication aids for the purposes of consultation of alerts, pursuant to Article 96 of the Schengen Convention, by the diplomatic and consular posts of certain Schengen States abroad.

At the meeting held on 22 May 1997, the Joint Supervisory Authority (hereinafter referred to as the JSA) decided on the basis of Articles 115 (3) and subparagraph f of Article 126 of the Schengen Convention, to send the following opinion to the Central Group on the subject of the problem contained in the heading:

- noting that the diplomatic and consular posts of certain Contracting Parties (e.g. Belgium, Spain, The Netherlands and France) use different technical means to facilitate local consultation of the alerts provided for in Article 96.

- since consultation takes place with a view to issuing visas to enter the Schengen territory in accordance with Articles 92 (1) in fine and Article 101 (2) of the Schengen Convention.

- since it is not always possible to directly search the SIS from the diplomatic and consular posts of certain Contracting Parties abroad, for various reasons.

The JSA has checked the compatibility of these posts with the original model for the SIS, as outlined in the Schengen Convention.

Several provisions in the Schengen Convention impose strict conditions on the procedures for using the SIS:

a. several passages under Article 92 provide for “an automated search procedure” (Article 92 (1) based on the “rapid and effective transmission” of data (Article 92 (2))

Article 92 (3): stipulates in addition that the technical support function, commonly known as the C.SIS, shall comprise a data file which shall ensure that the
data files of the national sections contain the same information "via on-line transmission".

Furthermore, Article 101 (2) of the Schengen Convention, authorizing different authorities to access alerts pursuant to Article 96, also refers to "searching such data directly", and specifically mentions the authorities responsible for issuing visas and central authorities responsible for examining visa applications.

The process of directly searching the system is mentioned again in Article 101 (4) and Article 102 (2) of the Schengen Convention and Article 106 (2) refers to the possibility of correcting or deleting data, i.e. amending or updating data "without delay", which each Contracting Party must comply with.

The various passages of Title IV of the Schengen Convention show that the system of processing information envisaged by the drafters of this Convention was an automated data search system enabling real-time data processing.

b. the Schengen Convention provides for several security measures.

Article 118 (1) requires each of the Contracting Parties to undertake a series of guarantees aiming to protect personal data contained in the SIS.

Among these, the JSA would like to highlight the following, in particular:

- measures to "prevent data media from being read, copied, modified, or removed by unauthorized persons" (control of data media) Article 118 (1b);

- measures to "guarantee that it is possible to check and establish what personal data has been entered into automated data processing systems, when and by whom" (control of transmission) Article 118 (1f);

- measures to "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) Article 118 (1h);

c. provision is also made for requirements to ensure monitoring of records

Article 103 of the Schengen Convention recommends that each Contracting Party ensure that every tenth transmission of personal data is recorded for the purposes of checking whether the search is acceptable or not.

In reply to a question from the Provisional Joint Supervisory Authority in January
1994 (see Note SCH/Aut-cont (94) 33 of 10 January 1994), the Steering Committee's representative said that the interpretation given to this article was that at least every tenth hit should be recorded (see Note SCH/OR-SIS (95) 116 of 16 June 1995).

On these grounds, the JSA is of the opinion that the use of duplication aids, in whatever form (CD Rom, diskette etc.) for the purposes of consultation of alerts provided for in Article 96 of the Convention by the diplomatic and consular posts of certain Schengen States abroad should fulfil the following three essential conditions:

1. The methods and means of duplication should guarantee that the data is identical, in real time, to processing of this data at the C.SIS. Any time difference, however small, should comply with the conditions provided for under 4.

2. These should guarantee at least the level of protection required in Article 118 (1) of the Schengen Convention and especially its subparagraphs b), d), f) and h); and should also comply with the condition laid down in Article 118 (3) of the Schengen Convention.

3. The programme on which they are based should enable records in accordance with the condition laid down in Article 103 of the Schengen Convention;

These records should be returned to the Schengen State every six months and made available to the national supervisory authority, provided for under Article 114 of the Schengen Convention, by the body with central responsibility for the national section of the SIS provided for under Article 108 (1) of the Schengen Convention;

4. In the event that duplication aids are used which run the risk of the data not being identical, the JSA urges that the Contracting Party, assumes its responsibility, as provided for in Articles 92 (2) and 116 of the Convention, as follows:

- where an alert exists for an individual in the duplicated aid used, the Contracting Party shall carry out a real time check (network, telephone, Fax) to confirm the accuracy of this information;

- where no alert exists for an individual in the duplicated aid used, the Contracting Party shall accept responsibility in the event that an alert is issued for the same individual in the space of time between the duplication
of the data and real time. This responsibility may only be removed subject to proof of a real-time check at the time of the visa application.
Joint Supervisory Authority

Brussels, 3 February 1998
SCH/Aut-cont (97) 55 rev 2
Translation: orig.: DE/FR

**OPINION 98/1 ON ARCHIVING DOCUMENTS AFTER THE ALERT HAS BEEN DELETED**

Re.: Archiving documents after the alert has been deleted

At its meeting of 3 February 1998, pursuant to Art 115(3) of the Schengen Convention implementing the Schengen Agreement (hereafter referred to as the Convention), the Joint Supervisory Authority adopted the following opinion:

Conscious that national police departments in certain Contracting Parties keep documents relating to alerts even after alerts issued pursuant to Article 95(1) of the Convention have been deleted and do so for the purpose of creating criminal records.

Aware that in order to do this the police authorities invoke provisions in national data protection law (see Point 2.1.3. b of the Sirene Manual), whereby the provisions of Title VI of the Convention shall also be applicable.

The Joint Supervisory Authority has studied these practices and underscores the following data protection requirements first and foremost.

The Joint Supervisory Authority confirms the fundamental principles and provisions laid down in the Convention with regard to data protection, in particular:

a. data may be supplied and used solely for the purposes laid down for the alert itself (Article 102(1) and Article 94(1) of the Convention). A derogation may only be made to this general principle if there is a need to prevent an imminent serious threat to law and order and safety or for serious reasons of State security or for the purposes of preventing a serious offence (Art. 102(3)).

b. Any use of data which does not comply with Article 102(1 to 4) shall be considered as misuse (Art. 102(5)).

c. Pursuant to Art. 112 of the Convention, personal data saved in the Schengen Information System for the purposes of locating persons shall be stored no longer than necessary for the intended purpose.
d. These basic principles shall apply by way of a complementary interpretation of legally binding texts for all types of data processing relating either directly or indirectly to alerts in the Schengen Information System.

The Joint Supervisory Authority therefore believes the following measures should be taken:

a. After an alert issued for the purpose of locating an individual has been deleted, every Contracting Party to the Schengen Convention shall, pursuant to Art. 112 of the Convention, destroy all its accompanying documents immediately.

b. The Schengen bodies shall revise the Sirene Manual with a view to deleting the provisions 2.1.3 b) which are incompatible with the Schengen Convention.
OPINION 98/2 ON ENTERING AN ALERT IN THE SCHENGEN INFORMATION SYSTEM
ON INDIVIDUALS WHOSE IDENTITY HAS BEEN USURPED

The JSA has examined the problems encountered as a result of the misuse of aliases by individuals who are the subject of an alert in the SIS (see notes SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 and SCH/Aut-cont (97) 42), in the light of the principles governing data protection laid down in the Schengen Convention.

In most states, alerts on individuals whose identity has been usurped are kept in the SIS. For the time being, it is not possible to specify in the SIS, at least using free text, that the alert concerns a usurped identity.

The JSA would hereby like to reiterate the following principles and fundamental rights with regard to data protection:

a. The data may be supplied and used solely for the purposes intended for each alert (Articles 102 (1) and Article 94 (1)); any derogation from this rule shall be exceptional and justified by the need to prevent an imminent serious threat or a serious offence (Article 102 (3)).

b. Any use of data which does not comply with paragraphs 1 to 4 shall be considered as misuse (Article 102 (5)).

c. The right of an individual who finds that data relating to their person is factually or legally inaccurate to have this information corrected or deleted (Article 110 (1)).

d. The right of an individual to bring an action before the courts or the authority competent under national law to correct or delete data in an alert relating to their person (Article 111 (1)).

e. The right of an individual to ask the supervisory authorities to check data in an alert relating to their person (Article 114 (2)).
The JSA, taking due and balanced account of the rights of the person whose identity has been usurped, provided for in the Schengen Convention, and the need to detect the usurper, hereby delivers the following opinion:

1. Entry of data in the SIS on individuals whose identity has been usurped shall be governed by national law, unless more stringent conditions are laid down in the Schengen Convention (Article 104 (1)).

2. The Contracting Party issuing the alert shall guarantee that data is entered solely for the specified purposes and that it is up-to-date and correct (Article 102 (1), Article 106 (1), Article 110, and the provisions relating to data protection laid down in the Council of Europe Convention (No. 108), inter alia those contained in Article 5, which are binding on the Schengen States).

3. The Contracting Party issuing the alert shall guarantee the right to correction or deletion of the data stored, in accordance with the procedure laid down in Article 106 of the Schengen Convention.

4. The question as to whether an alert on an individual whose identity has been usurped should be kept in the SIS needs to be carefully weighed up, bearing in mind on the one hand, the rights of the person whose identity has been usurped and on the other hand, the need to detect the usurper.

5. In the interim period until the SIS II is brought into service an appropriate, and if possible joint, solution should be sought and adopted so as to indicate that the alert is on an usurped identity. The JSA would be willing to cooperate to help find a solution of this nature.
b. In accordance with Article 102 (1) of the Convention, the Contracting Parties may only use the data for the purposes laid down for each type of alert;

In accordance with Article 102 (2) of the Convention, data may not be copied (unless for technical purposes, so that the competent authorities can carry out a direct search);

In accordance with Article 102 (4) of the Convention, data may not be used for administrative purposes;

Finally, in accordance with Article 102 (5) of the Convention, any use of data which does not comply with the abovementioned paragraphs of this article shall be considered misuse;

c. In accordance with Article 104 (1) of the Convention, national law shall apply to data entered in the national section of the SIS, unless more stringent conditions are laid down in the Convention;

d. In accordance with Article 126 (1) and (2) of the Convention, personal data provided for in the Convention may only be transmitted to those Contracting Parties which have adopted the national provisions required to achieve a level of protection of personal data at least equal to that provided for in the Council of Europe Convention No 108 of 28 January 1981;

e. In accordance with Article 118 (d), each Contracting Party shall undertake, in relation to the national section of the Schengen Information System, to adopt the requisite measures in order to prevent automated data processing systems from being used by unauthorized persons by means of data transmission equipment;

f. Data on the make, type, colour and technical features of a vehicle is not personal data, insofar as it cannot be linked to the identity of the person connected with this vehicle, for instance if the registration number or the chassis number could lead to the identification of the owner of the vehicle or its driver;

g. The police authorities of each country participating in the ASF project may exchange information (in this instance, personal data) from the national databases, provided that this exchange is permissible under bilateral or multilateral police cooperation instruments or is not prevented by national
OPINION 98/3 OF 3 FEBRUARY 1998 ON THE POSSIBILITY OF LINKING THE SCHENGEN INFORMATION SYSTEM AND THE INTERPOL ASF - STOLEN VEHICLES PROJECT

The JSA received a note from the German delegation to the SIS Steering Committee (document SCH/OR.SIS (97) 81) of 30 April 1997 outlining the ASF - stolen vehicles project (Automated Search Facility) with a view to Schengen's adopting a common position towards Interpol. This has led the JSA to question whether SIS data on persons and stolen vehicles can be sent to Interpol.

The abovementioned note contains a brief outline of the project: "According to the German delegation's information, only four countries are currently participating in the stolen vehicles project (Sweden, Luxembourg, Russia and Slovakia). Data is currently available on approximately 80,000 stolen vehicles. This data concerns persons and stolen vehicles."

Given that the above note also mentions the fact that this project is due to be extended to cover other categories of data (stolen works of art, credit cards, falsified documents and passports, stolen boats/planes), and the importance that these projects could take on in the future, the JSA has decided to deliver an opinion on this project, thus offering a response to the question of whether SIS data on persons and stolen vehicles can be transmitted to Interpol in connection with the ASF project.

With regard to personal data protection,

the JSA,

Whereas:

a. In accordance with Article 101 (4) of the Convention, only the competent authorities are authorized to directly search the data contained in the SIS. Each Contracting Party shall send the Executive Committee a list of these authorities, indicating for each of them which data it may search and for what
data protection legislation;

h. Account shall be taken of the opinion of 7 March 1997 delivered by the JSA on the pilot project on stolen vehicles (see document SCH/Aut-cont (97) 22 rev). This opinion involves determining whether a country which is not yet linked up to the Schengen Information System may have access to data on stolen vehicles contained in the SIS.

hereby delivers the following opinion:

1. Information and personal data contained in the Schengen Information System cannot be transmitted to Interpol in connection with the ASF - stolen vehicles project without breaching the provisions of the Convention, and in particular Articles 101, 102, 118 and 126.

2. Information on the make, type, colour and technical features of the vehicle is not personal data as such within the meaning of the Schengen Convention.

3. The transmission of information to Interpol as part of the ASF - stolen vehicles project does not breach the provisions on the protection of personal data contained in the Convention, insofar as the data cannot be linked to the identity of the person connected with the vehicle.

4. Police exchanges of information on stolen vehicles, taken from national files, are governed by the relevant national legislation, and more specifically legislation on data protection.
c. place, date and time of the search

d. Grounds for consultation, such as the legal basis for an alert.

3. In addition, the following are also desirable for checking the admissibility of data's being consulted in individual cases.

   The reference number or police day book number, if this exists, used for locating the relevant file.

4. The data shall only be used for the purposes laid down in Article 103.

5. Log data shall be deleted within six months.

The JSA insists that the obligation provided for in Article 103 of the Convention be upheld in accordance with this opinion.
RULES OF PROCEDURE
OF THE JOINT SUPERVISORY AUTHORITY
APPROVED BY THE JSA ON 2 FEBRUARY 1996 ARTICLE 2 OF WHICH
AMENDED BY WAY OF THE DECISION OF THE JSA MADE AT ITS MEETING OF 4
JULY 1997

The Joint Supervisory Authority,

Having regard to Article 115 of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of controls at the common borders, signed on 19 June 1990, hereinafter referred to as the "Convention";

Adopted the following Rules of Procedure on 19 October 1995:

ARTICLE 1 - TERMS OF REFERENCE

1. The Joint Supervisory Authority, in compliance with the present Rules of Procedure, shall carry out the tasks conferred upon it by virtue of the Convention, together with other tasks relating to the protection of personal data which it deems to be related to the implementation of the Convention.

2. In carrying out its tasks, the Joint Supervisory Authority may intervene either on its own initiative or at the request of the national supervisory authority of a Schengen Member State, a Contracting Party or a body of the Schengen System in compliance with the provisions of the Convention.

ARTICLE 2 - COMPOSITION

1. The Joint Supervisory Authority, in compliance with Article 115 of the Convention, shall be made up of two representatives of the national supervisory authority, referred to in Article 114 of the Convention, of each Contracting Party in which the Convention has entered into force in accordance with Article 140 of the Convention. A Contracting Party shall also be understood to mean a Party with which the Parties to the Schengen Agreement
and the Schengen Convention have concluded a cooperation agreement on the
abolition of controls on persons at the common internal borders, provided that
this cooperation agreement has been implemented.
Each delegation shall carry one vote.

2. The Joint Supervisory Authority may, upon unanimous decision, grant obser­
ver status without the right to vote to the representatives of the national supervisory authorities, referred to in Article 114 of the Convention, or to independent experts of the Contracting Parties who do not yet fulfil the conditions laid down in the final sentence of Article 140 (2) of the Convention. A Contracting Party shall also be understood to mean a Party with which the Parties to the Schengen Agreement and the Schengen Convention have concluded a cooperation agreement on the abolition of controls at internal borders as defined in Article 1 of the Schengen Convention, provided that this cooperation agreement has been ratified, accepted or approved by all Parties but has not yet entered into force.

3. Neither the members of the Joint Supervisory Authority nor the observers may sit on working groups or be members of an authority - other than the national supervisory authority for the protection of personal data - instituted under the Convention. They may be included in their national delegations as experts.

4. If a member of the Joint Supervisory Authority is unable to attend a meeting, he may be replaced by a person designated by the national supervisory authority in compliance with the present article.

5. Members of the Joint Supervisory Authority may be accompanied by an expert to assist them.

ARTICLE 3 - CHAIRMANSHP

1. The Joint Supervisory Authority shall elect from among its members a
Chairman and a Deputy Chairman: They shall be elected by a two-thirds
majority of the delegations referred to under Article 2 (1). They shall have a
one-year period of office renewable once.

2. The Deputy Chairman shall belong to a delegation other than that of the
Chairman; he shall replace the Chairman in the event of the Chairman’s being
absent or unable to attend.

3. Should a vacancy occur before the expiry of the period of office of the
Chairman or the Deputy Chairman, a substitute shall be elected. The
substitute elected shall perform his duties for the remainder of the period of office.

**ARTICLE 4 - ROLE OF THE CHAIRMAN**

1. The Chairman shall represent the Joint Supervisory Authority. He shall ensure its smooth running. He shall convene the Authority and set the venue, day and time of meetings. He shall call to order and adjourn the sessions. He shall lead the debates. The Chairman shall draw up the provisional agenda.

2. With a view to preparing for Joint Supervisory Authority deliberations, the Chairman may, for a specific subject, designate one or more rapporteurs from among the members.

**ARTICLE 5 - PROCEDURE**

1. The Joint Supervisory Authority shall meet at least twice a year. Meetings shall also be held on the initiative of the Chairman as well as whenever at least three delegations, as referred to under Article 2 (1), put in a reasoned request to this effect, either verbally during the meeting or in writing. Lastly, the JSA shall meet in the cases provided for in the Convention.

2. Except in cases deemed urgent by the Chairman, the notice convening a meeting shall be sent out at least a fortnight before the date of the meeting. The notice shall comprise the provisional agenda as well as, as far as possible, the necessary documents for the debates.

3. The Joint Supervisory Authority shall adopt the final agenda at the beginning of each meeting.

**ARTICLE 6 - QUORUM AND MAJORITY VOTING RULES**

1. Meetings of the Joint Supervisory Authority shall be valid only if at least two thirds of the delegations referred to under Article 2 (1) are present.

2. Except where there is provision in Article 13, the acts of the Joint Supervisory Authority shall be adopted if half plus one of the delegations present as referred to under Article 2 (1) are in favour.

3. Each delegation may deposit a note explaining its vote.

4. The Joint Supervisory Authority shall deliberate on the basis of documents and
drafts written in one of the national languages of all of the Schengen States.

**Article 7 - Openness and Recipients of Acts**

1. Except as otherwise decided by the Joint Supervisory Authority, its meetings shall not be public.

2. The Joint Supervisory Authority shall determine who is to be sent its acts and shall decide whether or not to make them public, without prejudice to the provisions of Article 115 (4) of the Convention.

**Article 8 - Written Procedure**

1. The acts of the Joint Supervisory Authority may be adopted by a written procedure, on condition that all the delegations have agreed to that procedure in principle during a meeting.

2. In the event of urgent matters, the Chairman may use the written procedure on his own initiative.

3. In either case, the Chairman shall send a draft to all members of the Joint Supervisory Authority. Any delegations who fail to send in their comments before a deadline, to be set by the Chairman, of at least one fortnight after the date of receipt of the draft, shall be deemed to have approved the draft.

4. The written procedure provided for under paragraph 2 of the present Article shall be terminated should a delegation, within five working days after the date of receipt of the draft, request that the draft be debated in the Joint Supervisory Authority.

**Article 9 - Working Groups, Experts, On-Site Verifications**

1. The Joint Supervisory Authority may institute working groups whose task it shall determine.

2. The Joint Supervisory Authority may call in experts. It may draw up a list of experts who shall be the first to be consulted.

3. As regards monitoring the technical support function, the Joint Supervisory Authority may designate one or more of its members to conduct on-site verifications. Should the Chairman consider the matter urgent, he may designate a member on his own initiative. In this case, he shall inform the
members of the Joint Supervisory Authority forthwith. The members designated to carry out verifications may be assisted by experts from the above-mentioned list.

4. The working groups, experts and Authority members instructed to conduct verifications shall report on the results of their missions to the Joint Supervisory Authority.

**ARTICLE 10 - SECRETARIAT**

1. The Secretariat of the Joint Supervisory Authority shall be assured under the responsibility of the Chairman by the personnel and services made available to it by the competent authority within Schengen cooperation.

2. The Secretariat shall maintain a register of the acts adopted by the Joint Supervisory Authority.

3. Correspondence to the Joint Supervisory Authority shall be addressed to the Secretariat, for the attention of the Chairman.

**ARTICLE 11 - MINUTES**

1. Minutes shall be drawn up for each meeting of the Joint Supervisory Authority.

2. The draft minutes shall be written by the Secretariat, under the responsibility of the Chairman. Minutes shall be submitted for approval by the Joint Supervisory Authority at the next meeting.

3. Members and observers may have the minutes rectified subsequently in accordance with the comments made by them during the relevant meeting.

**ARTICLE 12 - SECRECY**

Without prejudice to the application of Article 7 (2), members of the Joint Supervisory Authority, observers, experts and members of the Secretariat shall be bound to respect secrecy. This obligation does not apply vis-à-vis the national supervisory authorities or vis-à-vis the other national authorities to which members and observers have to report in compliance with their national laws.
ARTICLE 13 - AMENDMENTS TO THE RULES OF PROCEDURE

The Joint Supervisory Authority shall adopt provisions amending the present Rules of Procedure unanimously. Except where there is provision to the contrary, such proposals shall enter into force one week after their adoption.
COMPILATION NOTE

COMPOSITION OF THE JSA DELEGATIONS

BELGIUM

M. Thomas (until 19 January 1998)
Commission Vie Privee
Bld de Waterloo 115 - 1000 Bruxelles

M. B. De Schutter
Commissie bescherming persoonlijke levensfeer - V.U.B.
Vrije Universiteit Brussel
Pleinlaan 2
1050 Brussel
Tel: 629 21 11
Fax: 629 36 33

Mme B. Havelange
Ministère de la Justice - Commission Vie privée
Bld de Waterloo 115.- 1000 Bruxelles
Tel: 542 72 02
Fax: 542 72 12

THE NETHERLANDS

MM. P.J. Hustinx & P.A. Michael
Registratiekamer
Prins Clauslaan 20
Postbus 93374
25090AJ 's-Gravenhage
Tel: 00 31 70 381 13 00
Fax: 00 31 70 381 13 01

SPAIN

M. D. Juan Maria Bandres Molc
San Martin 13 4?  
20005 San Sebastian  
Tel: 00 34 43 42 24 70  
Fax: 00 34 43 43 10 61

M. Miguel Angel Lopez Herrero  
Agence de Protection des Données  
Paseo de la Castellana 41  
28046 Madrid  
Tel: 00 34 1 308 47 90  
Fax: 00 34 1 308 46 92

**GERMANY**

M. J. Jacob, member of the federal commission for data protection represented by:  
M. W. von Pommer Esche  
Head of Department at the federal commission for data protection  
Riemenschneiderstrasse, 11  
53175 Bonn (Bad Godesberg)  
Tel: 00 49 228 81 99 50  
Fax: 00 49 228 81 99 550

M. R. Hamm, member of the Hessen commission for data protection represented by:  
Mme A. Schriever-Steinberg, chef du département auprès du commissaire hessois à la protection des données  
Uhlandstr. 4  
65189 Wiesbaden  
Tel: 00 49 611 1408 0  
Fax: 00 49 611 37 85 79

M. A. Turk and Melle F. Fourets  
C.N.I.L.  
rue Saint Guillaume, 21  
75340 Paris Cédex 07  
Tel: 00 33 1 53 73 22 22  
Fax: 00 33 1 53 73 22 00

**PORTUGAL**

M. J.A.M. Labesca da Silva  
M. Nuno Albuquerque Morais Sarmento
Rua de S. Bento, 148 3º Andar
1200 Lisboone
Tel: 00 351 1 392 84 00
Fax: 00 351 1 397 68 32

LUXEMBOURG

M. R. Faber and M. S. Wagner, representatives
Secrétariat de la Commission
Ministère de la Justice
2934 Luxembourg
Tel: 00 352 478 45 46
Fax: 00 352 227 661

M. Jean Wagner and M. G. Wiwenes, alternate representatives

AUSTRIA

Mme W. Kotschy
Mme E. Souhrada-Kirchmayer
Ballhausplatz 1
A-1014 Wien
Österreich
Tel: 00 43 1 531 15/2525
Fax: 00 43 1 53 115/2690

ITALY

M. S. Neri
Tel 00 39 6 67 60 46 93
Fax 00 39 95 62 12 20
Fax 00 39 6 676 096 78

M. Buttarelli
Garante per la portezione dei dati personali
Via della Chiesa Nuova, 8 - 00186 Roma
Tel. 00 39 6 68 18 61
Fax 00 39 6 68 18 669

Greece

M. C. Dafermos
Tel. 00 301 779 58 05  
Fax 00 301 77 80 317  
suppléant: M. G. Deliyanis  
Tel. 00 301 89 46 451/32 28 056  
Fax 00 301 77 80 317

**ICELAND: OBSERVER**

Mr. S. Johannesdóttir  
Mr. T. Örlygsson

Data Protection Commission  
Ministry of Justice  
Armarhvoll  
150 Reykjavik - Islande  
Tel. 00 354 560 90 10  
Fax 00 354 552 73 40

**DENMARK: OBSERVER**

Ms. Lott N. JØRGENSEN  
Registertilsynet  
Christians Brygge 28 - 1559 KØBENHAVN V  
Danemark  
Tel. 00 45 33 14 38 44  
Fax 00 45 33 13 38 43

**SWEDEN: OBSERVER**

Ms. A. Bondestam  
General-Director  

Ms. B-M. Wester  
Administrative Officer  
Datanspektionen  
box 8114  
S-104 20 Stockholm - Sweden  
Tel. 00 46 8 657 61 00  
Fax 00 46 8 650 86 13
NORWAY: OBSERVER

Ms G. Slettemark
Datatilsynet
Postboks 8177 Dep. 0034 Oslo
Tel. 00 47 22 42 19 10
Fax 00 47 22 42 23 50

FINLAND: OBSERVER

Head of Finnish delegation: Mr. Aarnio
Ms. J. Meklin (>9th April 1998)
Ms. Maija Kleemola (<9th April 1998)
Office of the Data Protection Ombudsman
PL 315 Finland 00181 Helsinki
Tel. 00 358 9 18 251
Fax 00 358 9 18 25 783
RIGHT OF ACCESS AND COMMUNICATION TO INDIVIDUALS OF INFORMATION CONTAINED IN THE SCHENGEN INFORMATION SYSTEM CONCERNING THEM

SCHENGEN JOINT SUPERVISORY AUTHORITY

The Schengen Information System

Welcome to the Schengen area

National data protection authorities

The Schengen Information System

The Schengen Agreement and the Convention implementing the Agreement have led to the creation of an area of free movement of persons by abolishing controls at internal borders between the Member States and by introducing the principle of a single set of controls on entry to the Schengen territory. For security reasons, it has been necessary however to introduce compensatory measures, the most important of which is the Schengen Information System (SIS).

The SIS is a database which is used by all the Schengen Member States and brings together two main categories of information, firstly, data on wanted persons or persons under surveillance, and secondly, data on missing vehicles or objects.

For instance, the following may be recorded in the Schengen Information System:

- Wanted persons or persons under police surveillance.
- Missing person or persons who should be placed under protection, in particular minors.
- Non-Schengen nationals who are banned entry to the Schengen territory.
- Persons whose identity is fraudulently used as an alias by other persons.

The SIS is monitored by an independent body: the Schengen Joint Supervisory Authority (JSA). This authority, which is made up of members of the national authorities for the protection of personal data from the Schengen Member States, is responsible.
inter alia, for carrying out technical checks on the central database located in
Strasbourg and ensuring that the Member States uphold individuals' rights of
access enshrined in the Schengen Convention.

**YOUR RIGHTS VIS-À-VIS THE SIS**

The SIS directly concerns you, whether you are a national of a Schengen Member
State or not.

The Schengen Convention itself recognizes the rights of individuals. These
include:

- the right to access information concerning you which is contained in the SIS,
- the right to correct data, where there is a de jure or de facto mistake,
- the right to apply to the courts or competent authorities to demand that data be
corrected, deleted or that damages be awarded,
- the right to ask for data to be checked and to question the use made of such
data.

If you have reason to believe that your name appears in the SIS, do not hesitate to
exercise your rights. The national data protection authorities in the Schengen
Member States are there to provide you with any useful information you may
require to further your case.

Any checks on your alert in the SIS (to establish whether the reasons for your
inclusion in the SIS are founded and any personal data which concerns you) will
be carried out in accordance with the national legislation that applies in whichever
country you choose to exercise your rights. At your request, you will be sent
information on the national law applicable by the relevant national data protec-
tion authority, whose address can be found overleaf. You will then be informed of
the results obtained, or of the follow-up given to your request.

The Schengen
Information System
This leaflet is intended to answer your questions. Read it.

Official bodies are available to provide any further information you require.

JSA Secretariat
39, rue de la Regence
1000 Brussels
Tel. 00322 519 38 76
Fax. 00322 513 42 06

National data protection authorities

**FOR THE NETHERLANDS**

Registratiekamer
Tel. : 00 31 70 381 13 00
Fax : 00 31 70 381 13 01

**FOR GERMANY**

Der Bundesbeauftragte für den Datenschutz
Tel. : 00 49 228 81995-0
Fax : 00 49 228 81995-50

**FOR BELGIUM**

Commission de la protection de la vie privée
Commissie voor de bescherming van de persoonlijke levenssfeer
Tel. : 00 32 2 542 72 00
Fax : 00 32 2 542 72 12

**FOR AUSTRIA**
Datenschutzkommission  
Tel.: 00 43 1 53 115/2525  
Fax: 00 43 1 53 115/2690

**FOR LUXEMBOURG**

Autorité de contrôle  
"Système d'Information Schengen"  
Tel.: 00 352 478 45 62  
Fax: 00 352 225 296

**FOR FRANCE**

Commission Nationale de l'Informatique et des Libertés  
Tel.: 00 33 1 53 73 22 22  
Fax: 00 33 1 53 73 22 00

**FOR PORTUGAL**

Comissão Nacional de Protecção de Dados Pessoais Informatizados  
Tel.: 00 351 1 392 84 00  
Fax: 00 351 1 397 68 32  
e-mail: cnpdpi@mail.telepac.pt

**FOR SPAIN**

Agencia de Proteccion de Datos  
Tel.: 00 34 91 308 48 31/308 47 90  
Fax: 00 34 91 308 46 92

**FOR ITALY**

Garante per la protezione dei dati personali  
Tel.: 00 39 6 68 18 61  
Fax: 00 39 6 68 18 669

**FOR GREECE**
Authority for the protection of personal data
Tel.: 00 30 1 779 58 05
Fax: 00 30 1 77 80 317

Reference documents:

- The Schengen Agreement of 14 June 1985
- The Convention implementing the Schengen Agreement of 19 June 1990

These documents will be sent to you, on request, by the Secretariat of the Joint Supervisory Authority, whose address can be found overleaf.