CONVENTION

IMPLEMENTING THE SCHENGEN AGREEMENT

of 14 June 1985

TITLE IV

THE SCHENGEN INFORMATION SYSTEM

CHAPTER 1

ESTABLISHMENT OF THE SCHENGEN INFORMATION SYSTEM

Article 92

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

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

3. The Contracting Parties shall set up and maintain, on a common cost basis and bearing joint liability, the technical support function of the Schengen Information System. The French Republic shall be responsible for the technical support function, which shall be located in Strasbourg. The technical support function shall comprise a data file which will ensure via on-line transmission that the data files of the national sections contain identical information. The data files of the technical support function shall contain alerts for persons and property in so far as these concern all the Contracting Parties. The data file of the technical support function shall contain no data other than those referred to in this paragraph and in Article 113(2).

CHAPTER 2

OPERATION AND USE OF THE SCHENGEN INFORMATION SYSTEM

Article 93

The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public policy and public security, including national security, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system.

Article 94

1. The Schengen Information System shall contain only those categories of data which are supplied by each of the Contracting Parties, as required for the purposes laid down in Articles 95 to 100. The Contracting Party issuing an alert shall determine whether

the case is important enough to warrant entry of the alert in the Schengen Information System.

2. The categories of data shall be as follows:

(a) persons for whom an alert has been issued;

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

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

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

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

(c) first letter of second forename;

(d) date and place of birth;

(e) sex;

(f) nationality;

(g) whether the persons concerned are armed;

(h) whether the persons concerned are violent;

(i) reason for the alert;

(j) action to be taken.

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

4. Where a Contracting Party considers that an alert in accordance with Articles 95, 97 or 99 is incompatible with its national law, its international obligations or essential national interests, it may subsequently add to the alert contained in the data file of the national section of the Schengen Information System a flag to the effect that the action to be taken on the basis of the alert will not be taken in its territory. Consultation must be held in this connection with the other Contracting Parties. If the Contracting Party issuing the alert does not withdraw the alert, it shall continue to apply in full for the other Contracting Parties.

Article 95

1. Data on persons wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the requesting Contracting Party.

2. Before issuing an alert, the Contracting Party shall check whether the arrest is authorised under the national law of the requested Contracting Parties. If the Contracting Party issuing the alert has any doubts, it must consult the other Contracting Parties concerned.

The Contracting Party issuing the alert shall send the requested Contracting Parties by the quickest means possible both the alert and the following essential information relating to the case:

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

(b) whether there is an arrest warrant or other document having the same legal effect, or an enforceable judgment;

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

(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;

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

3. A requested Contracting Party may add to the alert in the data file of its national section of the Schengen Information System a flag prohibiting arrest on the basis of the alert until the flag is deleted. The flag must be deleted no later than 24 hours after the alert has been entered, unless the Contracting Party refuses to make the requested

arrest on legal grounds or for special reasons of expediency. In particularly exceptional cases where this is justified by the complex nature of the facts behind the alert, the above time limit may be extended to one week. Without prejudice to a flag or a decision to refuse the arrest, the other Contracting Parties may make the arrest requested in the alert.

4. If, for particularly urgent reasons, a Contracting Party requests an immediate search, the requested Contracting Party shall examine whether it is able to withdraw its flag. The requested Contracting Party shall take the necessary steps to ensure that the action to be taken can be carried out immediately if the alert is validated.

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

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

Article 96

1. Data on aliens for whom an alert has been issued for the purposes of refusing entry shall be entered on the basis of a national alert resulting from decisions taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.

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

This situation may arise in particular in the case of:

(a) an alien who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;

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

3. Decisions may also be based on the fact that the alien has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of aliens.

Article 97

Data on missing persons or persons who, for their own protection or in order to prevent threats, need temporarily to be placed under police protection at the request of the competent authority or the competent judicial authority of the Party issuing the alert shall be entered, so that the police authorities may communicate their whereabouts to the Party issuing the alert or may move the persons to a safe place in order to prevent them from continuing their journey, if so authorised by national law. This shall apply in particular to minors and persons who must be interned following a decision by a competent authority. The communication of data on a missing person who is of age shall be subject to the person's consent.

Article 98

1. Data on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation of liberty shall be

entered, at the request of the competent judicial authorities, for the purposes of communicating their place of residence or domicile.

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

Article 99

1. Data on persons or vehicles shall be entered in accordance with the national law of the Contracting Party issuing the alert, for the purposes of discreet surveillance or of specific checks in accordance with paragraph 5.

2. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:

(a) where there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences; or

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

3. In addition, the alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is clear evidence that the information referred to in paragraph 4 is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Contracting Party issuing the alert shall be obliged to consult the other Contracting Parties beforehand.

4. For the purposes of discreet surveillance, all or some of the following information may be collected and communicated to the authority issuing the alert when border checks or other police and customs checks are carried out within the country:

(a) the fact that the person for whom or the vehicle for which an alert has been issued has been found;

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

(c) the route and destination of the journey;

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

(e) the vehicle used;

(f) objects carried;

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

During the collection of this information steps must be taken not to jeopardise the discreet nature of the surveillance.

5. During the specific checks referred to in paragraph 1, persons, vehicles and objects carried may be searched in accordance with national law for the purposes referred to in paragraphs 2 and 3. If the specific check is not authorised under the law of a Contracting Party, it shall automatically be replaced, for that Contracting Party, by discreet surveillance.

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

Article 100

1. Data on objects sought for the purposes of seizure or use as evidence in criminal proceedings shall be entered in the Schengen Information System.

2. If a search brings to light an alert for an object which has been found, the authority which matched the two items of data shall contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Convention. The measures to be taken by the Contracting Party which found the object must be in accordance with its national law.

3. The following categories of objects shall be entered:

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

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

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

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

(e) issued identity papers (passports, identity cards, driving licences) which have been stolen, misappropriated or lost;

(f) banknotes (suspect notes).

Article 101

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

(a) border checks;

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

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

3. Users may only search data which they require for the performance of their tasks.

4. Each Contracting Party shall send the Executive Committee a list of competent authorities which are authorised to search the data contained in the Schengen Information System directly. That list shall specify, for each authority, which data it may search and for what purposes.

CHAPTER 3

PROTECTION OF PERSONAL DATA AND SECURITY OF DATA IN THE SCHENGEN INFORMATION SYSTEM

Article 102

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

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 101 to carry out a direct search. Alerts issued by other Contracting Parties may not be copied from the national section of the Schengen Information System into other national data files.

3. With regard to the alerts laid down in Articles 95 to 100 of this Convention, any derogation from paragraph 1 in order to change from one category of alert to another must be justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. Prior authorisation from the Contracting Party issuing the alert must be obtained for this purpose.

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

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

Article 103

Each Contracting Party shall ensure that, on average, every 10th transmission of personal data is recorded in the national section of the Schengen Information System by the data file management authority for the purposes of checking whether the search is admissible or not. The record may only be used for this purpose and shall be deleted after six months.

Article 104

1. Alerts shall be governed by the national law of the Contracting Party issuing the alert unless more stringent conditions are laid down in this Convention.

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

3. In so far as this Convention does not lay down specific provisions concerning performance of the action requested in the alert, the national law of the requested Contracting Party performing the action shall apply. In so far as this Convention lays down specific provisions concerning performance of the action requested in the alert, responsibility for that action shall be governed by the national law of the requested Contracting Party. If the requested action cannot be performed, the requested Contracting Party shall immediately inform the Contracting Party issuing the alert.

Article 105

The Contracting Party issuing the alert shall be responsible for ensuring that the data entered into the Schengen Information System is accurate, up-to-date and lawful.

Article 106

1. Only the Contracting Party issuing the alert shall be authorised to modify, add to, correct or delete data which it has entered.

2. If one of the Contracting Parties which has not issued the alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall advise the Contracting Party issuing the alert thereof as soon as possible; the latter shall be obliged to check the communication and, if necessary, correct or delete the item in question immediately.

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

Article 107

Where a person is already the subject of an alert in the Schengen Information System, a Contracting Party which enters a further alert shall reach agreement on the entry of the alert with the Contracting Party which entered the first alert. The Contracting Parties may also lay down general provisions to this end.

Article 108

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

2. Each Contracting Party shall issue its alerts via that authority.

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

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

Article 109

1. The right of persons to have access to data entered in the Schengen Information System which relate to them shall be exercised in accordance with the law of the Contracting Party before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 114(1) shall decide whether information shall be communicated and by what procedures. A Contracting Party which has not issued the alert may communicate information concerning such data only if it has previously given the Contracting Party issuing the alert an opportunity to state its position.

2. Communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties. In any event, it shall be refused throughout the period of validity of an alert for the purpose of discreet surveillance.

Article 110

Any person may have factually inaccurate data relating to them corrected or unlawfully stored data relating to them deleted.

Article 111

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

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

Article 112

1. Personal data entered into the Schengen Information System for the purposes of tracing persons shall be kept only for the time required to meet the purposes for which they were supplied. The Contracting Party which issued the alert must review the need for continued storage of such data not later than three years after they were entered. The period shall be one year in the case of the alerts referred to in Article 99.

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

3. The technical support function of the Schengen Information System shall automatically inform the Contracting Parties of scheduled deletion of data from the system one month in advance.

4. The Contracting Party issuing the alert may, within the review period, decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the technical support function. The provisions of paragraph 1 shall apply to the extended alert.

Article 113

1. Data other than that referred to in Article 112 shall be kept for a maximum of 10 years, data on issued identity papers and suspect banknotes for a maximum of five years and data on motor vehicles, trailers and caravans for a maximum of three years.

2. Data which have been deleted shall be kept for one year in the technical support function. During that period they may only be consulted for subsequent checking as to their accuracy and as to whether the data were entered lawfully. Afterwards they must be destroyed.

Article 114

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

of the national section of the Schengen Information System and for checking that the processing and use of data entered in the Schengen Information System does not violate the rights of the data subject. For this purpose, the supervisory authority shall have access to the data file of the national section of the Schengen Information System.

2. Any person shall have the right to ask the supervisory authorities to check data entered in the Schengen Information System which concern them and the use made of such data. That right shall be governed by the national law of the Contracting Party to which the request is made. If the data have been entered by another Contracting Party, the check shall be carried out in close coordination with that Contracting Party's supervisory authority.

Article 115

1. A joint supervisory authority shall be set up and shall be responsible for supervising the technical support function of the Schengen Information System. This authority shall consist of two representatives from each national supervisory authority. Each Contracting Party shall have one vote. Supervision shall be carried out in accordance with the provisions of this Convention, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, and in accordance with the national law of the Contracting Party responsible for the technical support function.

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

3. The joint supervisory authority shall also be responsible for examining any difficulties of application or interpretation that may arise during the operation of the Schengen Information System, for studying any problems that may occur with the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of the right of access to the system, and for drawing up harmonised proposals for joint solutions to existing problems.

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

Article 116

1. Each Contracting Party shall be liable in accordance with its national law for any injury caused to a person through the use of the national data file of the Schengen Information System. This shall also apply to injury caused by the Contracting Party which issued the alert, where the latter entered factually inaccurate data or stored data unlawfully.

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

Article 117

1. As regards the automatic processing of personal data communicated pursuant to this Title, each Contracting Party shall, no later than the date of entry into force of this Convention, adopt the necessary national provisions in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in accordance with Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector.

2. The communication of personal data provided for in this Title may not take place until the provisions for the protection of personal data as specified in paragraph 1 have entered into force in the territories of the Contracting Parties involved in such communication.

Article 118

1. Each Contracting Party undertakes, in relation to its national section of the Schengen Information System, to adopt the necessary measures in order to:

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control).

2. Each Contracting Party must take special measures to ensure the security of data while they are being communicated to services located outside the territories of the Contracting Parties. Such measures must be notified to the joint supervisory authority.

3. For the processing of data in its national section of the Schengen Information System each Contracting Party may appoint only specially qualified persons who have undergone security checks.

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

CHAPTER 4

APPORTIONMENT OF THE COSTS OF THE SCHENGEN INFORMATION SYSTEM

Article 119

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

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