ISSN 1725-2423

C 38

Volume 46

of the European Union

Official Journal

17 February 2003

| English edition | Information and Notices | |
|-----------------|-------------------------|-----|
| | | |
| Notice No | Contents | Pag |
| | I Information | |
| | Council | |
| 2003/C 38/01 | Sirene Manual | 1 |



I

(Information)

COUNCIL

SIRENE MANUAL (1)

(2003/C 38/01)

CONTENTS

| | | Page |
|--------|--|------|
| TITLE | — GENERAL | 4 |
| Introd | oction | 4 |
| 1. | The legal foundations | 5 |
| 2. | How the Sirene Bureaux are organised | 8 |
| 2.1. | The technical resources | 8 |
| | 2.1.1. The provisions for supplying information | 8 |
| | 2.1.2. The means of communication | 9 |
| | 2.1.3. Archiving the information | 9 |
| 2.2. | The service constraints | 9 |
| | 2.2.1. The deadlines for processing files | 9 |
| | 2.2.2. Availability of the Sirene Bureaux | 9 |
| TITLE | — ACTION | 9 |
| 3. | Areas of intervention | 9 |
| 3.1. | The main areas of intervention | 9 |
| | 3.1.1. The exchange of information prior to an alert | 9 |
| | 3.1.2. The exchange of information whilst entering an alert | 10 |
| | 3.1.3. The exchange of information for multiple alerts | 10 |
| | 3.1.4. The exchange of information when adding a flag | 10 |
| | 3.1.5. The exchange of information after a hit | 10 |
| | 3.1.6. The exchange of information for aliens not to be admitted | 10 |

⁽¹⁾ Council Decision 2003/19/EC of 14 October 2002 on declassifying certain parts of the Sirene Manual adopted by the Executive Committee established by the Convention implementing the Schengen Agreement of 14 June 1985 (OJ L 8, 14.1.2003, p. 34).

| | 3.1.7. | The exchange of information when the procedures following a hit cannot be followed | 11 |
|------|---------|---|----|
| | 3.1.8. | The exchange of information if the original objective is changed | 11 |
| | 3.1.9. | The exchange of information if data or found to be legally or factually flawed | 11 |
| | 3.1.10. | The exchange of information on the right to access and rectify data | 11 |
| 3.2. | Areas f | or supplementary intervention | 11 |
| | 3.2.1. | The exchange of information on police cooperation | 11 |
| | 3.2.2. | Specific powers in policing and security matters | 12 |
| | 3.2.3. | Overlapping roles of Sirene and Interpol | 12 |
| 4. | The pr | ocedures to be followed | 13 |
| 4.1. | The exc | change of information prior to an alert | 13 |
| | 4.1.1. | Checking whether the national law of the Contracting Parties authorises provisional arrest with a view to extradition | 13 |
| | 4.1.2. | Consulting the Contracting Parties for alerts on grounds of State security | 14 |
| 4.2. | Exchan | ge of information whilst entering an alert | 15 |
| | 4.2.1. | Sending a dossier for provisional arrest with a view to extradition | 15 |
| 4.3. | The exc | change of information for multiple alerts | 15 |
| | 4.3.1. | Checking for multiple alerts on an individual | 17 |
| | 4.3.2. | Checking for multiple alerts on a vehicle | 17 |
| | 4.3.3. | Negotiating entering a new alert if it is incompatible with a previous alert | 18 |
| 4.4. | The exc | change of information when adding a flag | 18 |
| | 4.4.1. | Consulting the Contracting Parties with a view to adding a flag | 18 |
| | 4.4.2. | A request for a flag to be added | 19 |
| | 4.4.3. | Systematic request for a flag to be added for a State's nationals | 19 |
| 4.5. | The exc | change of information after a hit | 19 |
| | 4.5.1. | Communicating the Schengen partners if an alert is discovered | 19 |
| | 4.5.2. | Communicating further information | 19 |
| 4.6. | The exc | change of information on aliens not to be granted admission | 20 |
| | 4.6.1. | Issuing residence permits or visas | 20 |
| | 4.6.2. | Refusing admission or expulsion from Schengen territory | 20 |
| 4.7. | The exc | change of information when the procedures following a hit cannot be executed | 21 |
| | 4.7.1. | Informing the alerting Contracting Party that the procedures cannot be followed | 21 |
| 4.8. | The exc | change of information if the objective of the alert is changed | 21 |
| | 4.8.1. | Informing the alerting Contracting Party that the objective has been changed | 21 |
| | 4.8.2. | Procedures for changing the original objective | 21 |

| 4.9. | The exc | schange of information in the case of inaccurate or inadmissible data | 21 |
|-------|---------|--|----|
| | 4.9.1. | Informing the alerting Contracting Party that data is inaccurate of inadmissible | 21 |
| | 4.9.2. | Rectification procedures | 22 |
| 4.10. | The exc | schange of information regarding the right to access or rectify data | 22 |
| | 4.10.1. | . Informing the national authorities of a request to access or rectify data | 22 |
| | 4.10.2. | 2. Information on requests for access for alerts issued by other Contracting Parties | 22 |
| | 4.10.3. | B. Information on access and rectification procedures | 22 |
| 5. | The ta | asks to be performed per alert category | 22 |
| 5.1. | Creatin | ng an alert | 22 |
| | 5.1.1. | The tasks common to all categories | 22 |
| | 5.1.2. | Measures to be taken for each individual category of alert | 23 |
| | | 5.1.2.1. Alerts pursuant to Article 95 | 23 |
| | | 5.1.2.2. Alerts pursuant to Article 96 | 23 |
| | | 5.1.2.3. Alerts pursuant to Article 97 | 23 |
| | | 5.1.2.4. Alerts pursuant to Article 98 | 23 |
| | | 5.1.2.5. Alerts pursuant to Article 99(2) | 23 |
| | | 5.1.2.6. Alerts pursuant to Article 99(3) | 23 |
| | | 5.1.2.7. Alerts pursuant to Article 100 | 23 |
| 5.2. | Amend | ding an alert | 23 |
| | 5.2.1. | Entering an alias | 23 |
| | 5.2.2. | Changing the grounds or procedures for an alert | 24 |
| 5.3. | Deletin | ng an alert | 24 |
| | 5.3.1. | Deleting after a hit | 24 |
| | 5.3.2. | Deleting when the conditions for maintaining the alert cease to be met | 24 |

SIRENE

SUPPLEMENTARY INFORMATION REQUEST AT THE NATIONAL ENTRIES

TITLE I

GENERAL

Introduction

On 14 June 1985, five countries (the Kingdom of Belgium, the Federal Republic of Germany, the French Republic, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands) signed an agreement at Schengen, a small town in Luxembourg, with a view to enabling '(...) all nationals of the Member States to cross internal borders freely (...) and to enable the free circulation of goods and services'.

One of the conditions for applying this agreement was that abolishing internal borders should not jeopardise State security. This means that all of the territories of the Contracting Parties have to be protected.

Several specialised groups were empowered to study practical measures so as to avoid security shortcomings once the agreement was brought into force.

The practical outcome of this work can be found in two documents, one technical (the feasibility study), and the other legal (the Convention).

The feasibility study, put to the Ministers and Secretaries of State of the five signatory countries of the Agreement in November 1988, lays down the broad technical principles for setting up the Schengen Information System.

The study not only sets out the structure of the information system, but also gives the essential specifications on the way it is to be organised to ensure it functions properly. This structure has been given the name 'Sirene', which is an acronym of the definition of the structure in English: Supplementary Information REquest at the National Entries.

This is in fact a summary description of a procedure for transmitting the supplementary information required by an end-user for further action when the SIS has been consulted and a hit established.

The five founder countries signed the Convention implementing the Schengen Agreement on 19 June 1990, and were later joined by Italy on 27 November 1990, Spain and

Portugal on 25 June 1991, Greece on 6 November 1992, Austria on 28 April 1995 and by Denmark, Sweden and Finland on 19 December 1996. The Convention lays down all of the legal rules binding on all of the Contracting Parties. Norway and Iceland also concluded a Cooperation Agreement with the Contracting Parties on 19 December 1996.

The common procedures and rules for cooperation between the partners are also detailed. Title IV focuses exclusively on the Schengen Information System.

The Schengen Information System (SIS) should provide the authorities responsible for:

- (a) border controls;
- (b) carrying out and coordinating the other police and customs checks within the country;
- (c) issuing visas, residence permits and for administrative matters relating to aliens;

access to alerts on persons, vehicles and objects, by means of an automated consultation procedure.

The SIS is made up of two separate components: one is the central system, and the other is the national systems (one for each country). The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system (C.SIS).

However, it should nevertheless be possible for the Contracting Parties to exchange the supplementary information required for implementing certain provisions foreseen under the Convention, and for the SIS to function properly, either on a bilateral or multilateral basis.

If each National Schengen Information System (N-SIS) is to meet the operating constraints set out in the feasibility study and the Convention, they must therefore have this supplementary information which is indispensable for using the Sirene computer system.

This is the technical operational service that will be used for transmitting all supplementary information requests at the national entries.

The following principle has been adopted:

A 'national Sirene Bureau' shall be set up by each of the Contracting Parties to serve as a single contact point for the other partners, available around the clock.

The legal foundations, the cases when action ought to be taken, the procedures to be followed and the general principles for organising the Sirene Bureaux are defined by all of the Contracting Parties so as to have common rules.

The arrangements agreed at international level to this end are recorded in this 'Sirene Manual'.

Should the Contracting Parties deem necessary, they may decide to amend or update the manual.

1. The legal foundations

Article 108(1) to (4), constitutes the legal basis for the very existence of the Sirene Bureaux and for any action taken by them.

The Sirene Bureaux should therefore exchange information at least regarding the SIS. Depending on decisions taken at national level, *inter alia* based on Articles 39 and 46 of the Convention, the Sirene Bureaux may also exchange any other information with the competent bodies that the other Contracting Parties have appointed for this type of information.

This exchange of information is governed by the provisions of Title VI of the Convention (Articles 126 to 130).

The Bureaux shall not transmit information on applications for asylum, for instance.

This general framework for the objectives of the Sirene Bureaux tasks should be completed by listing the articles of the Convention which in any way have an impact on their activities.

— Article 5:

- '1. For visits not exceeding three months, aliens fulfilling the following conditions may be granted entry into the territories of the Contracting Parties:
- (d) the aliens shall not be persons for whom an alert has been issued for the purposes of refusing entry.'

— Article 25:

1. Where a Contracting Party considers issuing a residence permit to an alien for whom an alert has been

issued for the purposes of refusing entry it shall first consult the Contracting Party issuing the alert and shall take account of its interests: the residence permit shall be issued only for serious reasons, in particular of a humanitarian nature or reasons arising from international obligations.

If a residence permit is issued, the Contracting Party issuing the alert shall withdraw the alert but may put the alien concerned on its national list of alerts.

2. Where it emerges that an alien who holds a valid residence permit, issued by one of the Contracting Parties, has been issued an alert for the purposes of refusing entry, the Contracting Party issuing the alert shall consult the Party which issued the residence permit in order to determine whether there are sufficient grounds for withdrawing the said residence permit. If the residence permit is not withdrawn the Contracting Party issuing the alert shall withdraw the alert but may put the alien in question on its national list of alerts.'

Article 39:

'1. The Contracting Parties undertake to ensure that their police authorities, in compliance with national legislation and within the scope of their powers, assist each other for the purposes of preventing and detecting criminal offences, insofar as national law does not stipulate that the request has to be made via the judicial authorities and provided that the request or the implementation thereof does not involve the application of measures of constraint by the requested Contracting Party. Where the requested police authorities do not have the power to deal with a request, they shall forward it to the competent authorities.'

— Article 46:

- 1. In certain cases, each Contracting Party may, in compliance with its national legislation and without being asked, send the Contracting Party concerned any information which may be of interest to it in helping prevent future crime and offences against or threats to public policy and security.
- 2. Information shall be exchanged, without prejudice to the arrangements for cooperation in border areas referred to in Article 39(4), via a central body to be designated. In particularly urgent cases, the exchange of information within the meaning of this Article may take place directly between the police authorities concerned, unless national provisions stipulate otherwise. The central body shall be informed of this as soon as possible.'

— Article 94:

- '1. The Contracting Party entering an alert shall determine whether the case is important enough to warrant the inclusion of the alert in the Schengen Information System.
- 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 note to the effect that the action referred to in connection with the alert will not be taken in its territory. Consultation must be held in this connection with the other Contracting Parties (...).'

— Article 95:

'2. Prior to 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, by the quickest means possible, to the requested Contracting Parties both the alert and essential information (...) on the case.

- 3. A requested Contracting Party may add to the alert in the file of the national section of the Schengen Information System a note prohibiting arrest in connection with the alert (...). The note shall 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. (...) the above time limit may be extended to one week. (...)
- 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 note. The requested Contracting Party shall take the necessary steps to ensure that the action to be taken can be carried out immediately, once the alert is validated.'

— 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 made in accordance with the rules of procedure laid down by national legislation, the administrative authorities or courts responsible.'

— Article 97:

'Information on missing persons or persons who, in the interest of protection or in order to prevent threats, need to be temporarily placed under police protection at the request of the competent authority or the competent judicial authority of the Party issuing the alert, shall be included 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 legislation. This shall apply in particular to minors and persons who must be interned following a decision by a competent authority. Communication of the information shall be subject to the consent of the missing person, if this person is of age.'

— Article 98:

- 1. Information on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for offences for which they are being prosecuted, or persons who are to be notified of a criminal judgment or of a summons to appear in order to serve a custodial sentence, shall be included, at the request of the competent judicial authorities, for the purposes of communicating their place of residence or domicile.
- 2. Information requested shall be communicated to the requesting Party in accordance with national legislation and the conventions on mutual assistance in criminal matters in force.'

— Article 99:

- '3. (...) an alert may be issued (...) at the request of the authorities responsible for State security. (...) The Contracting Party issuing the alert shall be required to consult the other Contracting Parties beforehand.
- 6. A requested Contracting Party may add to the alert in the file of the national section of the Schengen Information System a note prohibiting (...) performance of the action to be taken (...) The note 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 (...).'

— Article 100:

'2. If a search brings to light the existence of an alert on an item which has been found, the authority which matched the two shall contact the authority which issued the alert in order to agree on the requisite measures to be taken (...)'.

— Article 101:

- '1. Access to data contained 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 the administration of aliens within the framework of the application of the provisions of this Convention on 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 in order to fulfil their tasks.
- 4. Each of the Contracting Parties shall send the Executive Committee a list of the competent authorities which are authorised to directly search the data contained in the Schengen Information System. This list shall provide each authority with information on which data it may search and for what purposes.'

— Article 102:

'3. As regards the alerts laid down in Articles 95 to 100 of this Convention, any derogation (...) to change from one type of alert to another must be justified (...). Prior authorisation from the Contracting Party issuing the alert must be obtained for this purpose.'

— Article 104:

'3. Insofar as this Convention does not lay down specific provisions on the enforcement of the action requested in the alert, the national legislation of the requested Contracting Party carrying out the action shall apply. Insofar as this Convention lays down specific provisions on carrying out the action requested in the

alert, responsibility for the action to be taken shall be governed by the national law of the requested Contracting Party. If the requested action cannot be carried out, 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:

- '2. If one of the Contracting Parties which has not issued the alert has good reason to believe that a piece of information is legally or factually incorrect, it shall advise the Contracting Party issuing the alert thereof as soon as possible: the latter shall be obliged to check the information and, if necessary, correct or delete the item in question without delay.
- 3. If the Contracting Parties are unable to reach agreement, the Contracting Party which did not issue the alert shall submit the case to the joint supervisory authority (...) for its opinion.'

— Article 107:

'Where a person has already been 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 Party may also lay down general provisions to this end.'

— Article 108:

- '1. Each of the Contracting Parties shall designate an authority which shall have central responsibility for the national section of the Schengen Information System.
- 2. Each of the Contracting Parties shall enter its alerts via that authority.
- 3. The said authority shall be responsible for the correct operation of the national section of the Schengen Information System and shall take the requisite 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 contained in the Schengen Information System which relates to them shall be exercised in accordance with the law of the Contracting Party before which they invoke that right. If national legislation 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 person concerned shall be refused if there is a danger of it undermining the fulfilment of the legal task specified in the alert, or in order to protect the rights and freedoms of others. In any event, it shall be refused throughout the period of validity of the alert so that discreet surveillance may be carried out.'

— Article 110:

'Anyone who finds that data relating to their person is factually or legally inaccurate may have this information corrected or deleted.'

Analysing these articles of the Implementing Convention has made it possible to determine the main cases where Sirene intervention is called for. These principal cases have been completed according to the technical imperatives of the information systems and the degree of operational efficiency as defined jointly.

2. How the Sirene Bureaux are organised

The national Sirene Bureaux are the only contact points between the Contracting Parties in matters relating to the Schengen Information System.

In most cases, though, they are only intermediaries that forward the information to the competent national authorities. As such they merely carry out technical and formal controls. For other cases, the jurisdiction of the Sirene Bureaux must be defined at national level.

The officers responsible for the national files and users' services must vouch that the alerts entered in the SIS and the information transmitted by Sirene are accurate, up-to-date and legal. This constraint is the outcome of the combined impact of Articles 105 and 108 of the Convention.

The Sirene Bureaux are merely operators acting on behalf of their country in the course of international contact, as a legal and/or functional entity, in accordance with the rules established by each State.

Each Contracting Party decides how its Sirene is to be organised and what the national procedures are to be, whilst respecting the rules set out in this manual.

However, these national structures should be well-known to all of the Contracting Parties, and must comprise certain technical resources and service constraints common to all of the Contracting Parties.

The officers in charge of the Sirene Bureaux shall meet at least twice a year to assess how their services are cooperating, to take the technical measures required in the event of any disfunctioning and adjust procedures.

2.1. The technical resources

For the main, the technical resources are the modes of communicating information between the Sirene Bureaux. It should be borne in mind that messages may be transmitted orally, in writing and by image.

Each Sirene Bureau shall use the national part of the communication system defined by all of the Contracting Parties.

Common provisions, as given in Annex 1 to this manual, shall summarise the cases when a communication shall be in writing and the cases when it need only be verbal.

2.1.1. The provisions for supplying information

The following measures have been adopted:

- (a) the most appropriate means of communication must be determined on a case-by-case basis, according to technical possibilities and the requirements that the communication has to meet. Should circumstances dictate, the communications shall not be sent in unscrambled form:
- (b) the messages will be conveyed mainly by telephone. So as to keep written messages to a minimum, telephone conversations will not automatically be confirmed in writing. The criteria for transmitting messages are detailed in annex 1;
- (c) written messages shall be divided into two categories: free texts and standard forms that have to respect the instructions under Annex 5. If need be, the Sirene operators shall follow the transliteration rules set out for the SIS (see Annex 2). Preference should be given to using a language common to the Sirene operators who are in direct contact with one another when processing a case, so as to make it easier and quicker to use the information;

(d) The heads of the Sirene must have an e-mail address independent of the operating system. These specific addresses in the communication system shall enable direct mail exchange between the various Sirene heads.

2.1.2. The means of communication

The following measures have been adopted:

(a) the texts and images should preferably be sent via the specific mail channels defined by all of the Contracting Parties, rather than via telex, teletext, fax.

2.1.3. Archiving the information

The following measures have been adopted:

(a) each Contracting Party shall determine the provisions for storing information.

The Sirene Bureau of the Contracting Party issuing the alert is obliged to keep all of the information on its own alerts available to the other Contracting Parties.

The archives of each Sirene Bureau should be organised in such a way as to enable swift access to the relevant information in order to be able to meet very short deadlines for transmitting information;

(b) the files and other messages sent by the other Contracting Parties shall be stored according to procedures provided for under national law on data protection and on personal data as applicable in the receiving country. The provisions of Title VI of the Convention shall also apply. As far as is possible, these additional pieces of information should not be kept by the Sirene's once the corresponding alert has been erased.

2.2. Service constraints

Schengen Information System users may at any moment require further information so as to be able to implement a course of conduct. Operating constraints common to all Sirene Bureaux are therefore required.

2.2.1. Deadlines for processing files

The following measures have been adopted:

(a) the Sirene must answer requests for information made by the other contracting parties as soon as possible. The response must be given within 12 hours.

2.2.2. Availability of the Sirene Bureaux

The following measures have been adopted:

- (a) the Sirene Bureaux must operate 24 hours a day, every day of the year;
- (b) the international means of communication must be kept open permanently.

TITLE II

ACTION

3. Areas of intervention

Sirene action is to enable:

- the transmission of information on alerts in the Schengen Information System,
- adherence to the relevant provisions in the Convention,
- liaison between the national services and the international bodies responsible for public security assignments within the scope granted to them by each of the States.

These three general criteria for action have been summarised in the list of cases requiring intervention given below.

3.1. The main areas of intervention

3.1.1. The exchange of information prior to an alert (the second sentence of Article 95(2) and Article 99(3))

Two categories of alert come under this procedure: those under Article 95(2) (2nd sentence) on provisional arrest pending extradition and those under Article 99(3) on discreet surveillance or specific checks for State security purposes.

So as to guarantee that the procedure foreseen under Article 99(3) is followed, each Contracting Party shall take adequate technical or organisational measures to prevent an alert in this category from being entered into the Schengen Information System without the Sirene Bureau of that Contracting Party having been informed.

3.1.2. Information exchanged whilst entering an alert (Article 95(2))

This information is stipulated under the second part of the procedure foreseen by Article 95(2). A file should be sent containing information to supplement that already in the SIS. It should be forwarded to the other Contracting Parties and the information should be sent on a standard form.

See comments at point 4.1.1.

3.1.3. The exchange of information for multiple alerts (Article 107)

The existence of several alerts that have been issued by different countries for one and the same individual may cause confusion.

It is essential that the local police, who are the end-users of the Schengen Information System, are not faced with several types of procedure to follow that are contradictory. It is important that the police at local level know exactly what measures need to be taken.

A procedure should be established for detecting multiple alerts and there should be rules on setting priorities for entering them into the SIS.

This calls for:

- checks before entering an alert, to determine whether the individual is already in the SIS,
- consultation with the other Contracting Parties, if need be, if there are multiple alerts that are incompatible.

3.1.4. The exchange of information when adding a flag (Articles 94, 95, and 99)

Articles 94(4), 95(3) and 99(6) enable a requested Contracting Party to refuse to execute the prescribed procedure on its territory, and do so either temporarily or definitively. This option may be taken for alerts issued by virtue of Articles 95, 97 or 99.

Should this possibility be taken up, the alerts should be studied thoroughly immediately and a swift response should be given on the steps to be taken.

3.1.5. The exchange of information after a hit (Articles 95, 96, 97, 98, 99 and 100)

When an end-user consults the SIS on an alert and confirms that it matches the person, vehicle or object concerned, this positive response is termed as a hit.

The end-user might require supplementary information so as to be able to implement the procedures foreseen in the SIS tables 4, 10 or 16 under the best possible conditions (see Annex 4).

Unless stated otherwise, the issuing Contracting Party must be informed of the outcome of this hit.

This is primarily an operational matter, although it also has technical implications, as the alert then has to be processed. It might need to be erased, meaning another alert previously omitted from the system can be entered.

These alert 'management' activities are absolutely essential for the smooth functioning of the SIS.

3.1.6. The exchange of information for aliens not to be granted entry (Articles 5, 25 and 96)

The information on aliens on whom an alert has been issued, with a view to refusing entry in accordance with Article 96, covers two types of action:

- firstly to refuse these aliens access to Schengen territory, and to this end to take the necessary steps to ensure that the consular services of the Contracting Parties do not issue them a visa, if one is required, and that the external border control services refuse them entry into the territories of the Parties,
- secondly, if these aliens are already on Contracting Party territory, action is to be taken to prevent the services responsible from issuing them residence permits and to initiate proceedings for their expulsion.

To this end and to gain a better understanding of the origins and validity of the non-admission measure on the basis of which an alert was entered pursuant to Article 96, the Contracting Party in whose territory the third country national subject to the alert is intercepted asks the Contracting Party issuing the alert for the following information under heading 089 of form G:

- 1. Type of decision
- 2. Authority issuing the decision
- 3. Date of decision
- 4. Date of service
- 5. Date of enforcement
- 6. Date of expiry of decision or length of validity.

See also point 4(6)2.

The notification foreseen under Article 5(2) and the consultation foreseen under Article 25 fall within the jurisdiction of the authorities responsible for issuing residence permits or visas.

The Sirene Bureaux should not be involved in the procedures foreseen under these two articles except for transmitting supplementary information directly relating to the alerts (notification of a hit, clarification on identity, for instance) or in erasing alerts.

In addition, the Sirene Bureaux may be involved in transmitting supplementary information necessary for expulsion or for refusing an alien entry, or in transmitting information generated by these operations.

The Sirene Bureaux are used as central authorities for transmitting and receiving additional information during the consultation procedure provided for in Article 25(1) and (2).

For this purpose, the Sirene Bureaux exchange N and O forms (Article 25(1) and Article 25(2)) at the request of the authorities responsible for issuing residence permits or visas with a view to retaining or deleting the alert.

If the State which granted the residence permit discovers that the holder of the said permit is the subject of an alert issued by another State pursuant to Article 96 of the Schengen Convention, it shall inform the latter's Sirene Bureau (by fax, M form, etc.). The Sirene Bureau of the State which issued the alert shall then instigate the consultation procedure pursuant to Article 25(2) of the Convention using the form provided for this purpose.

If a third State (i.e. a State which neither granted the residence permit nor issued the alert for the holder of the permit) discovers that there are grounds for consultation, it shall notify both the State which issued the alert and the State which granted the residence permit.

3.1.7. The exchange of information when the procedures following a hit on an alert cannot be followed (Article 104(3))

Article 104(3) foresees procedure if a Contracting Party is unable, either by law or de facto, to follow procedure required by an alert.

3.1.8. The exchange of information if the original objective is changed (Article 102(3))

Article 102(3) allows for the purpose of the initial alert not to be respected after a hit in terms of how the data are to be used.

This procedure may only be used on grounds of the need to prevent an imminent serious threat to public order and safety, for serious reasons of State security or for the purposes of preventing a serious criminal offence.

The objective of the alert may only be altered subject to prior authorisation having been obtained from the issuing Contracting Party.

3.1.9. The exchange of information if data are found to be legally or factually flawed (Article 106)

The principle of data ownership laid down in Article 106 should not prevent a legal or factual error from being rectified. Paragraphs 2 and 3 of this Article covers this eventuality.

3.1.10. The exchange of information on the right to access and rectify data (Articles 109 and 110)

Any individual is entitled to have access to data on him/herself and, if need be, request that errors (whether de facto or legal) be corrected.

This possibility may be taken up in compliance with national legislation applicable in the country in which it is brought to bear.

A contracting Party may not authorise access to an alert issued by another Contracting Party unless the former has given the latter the opportunity to express its position.

3.2. Areas for supplementary intervention

3.2.1. The exchange of information on police cooperation (Articles 39 and 46)

Cooperation between the Contracting Parties and policing methods shall not be limited to using the information in the Schengen Information System alone.

Matching an alert may lead to the discovery of an offence or of a serious threat to public policy or to public security and there may also be a need to identify a person or object accurately.

The exchange of information, for instance, by means of photographs or finger prints may turn out to be indispensable. Articles 39 and 46 authorise these procedures for action.

This information shall be exchanged in such a way that complies with the provisions of Title VI of the Convention.

The following are recommended:

(a) the Sirene Bureaux of the Contracting Parties can exchange any useful information whilst respecting national measures taken to implement Articles 39 and 46;

(b) the Sirene Bureaux shall keep the other bureaux informed of measures taken at national level by each Contracting Party, as well as of any amendments made thereafter.

3.2.2. The specific powers in policing and security matters (Title III)

Title III of the Convention implementing the Schengen Agreement contains a number of innovative provisions in police and judicial cooperation. The Sirene Bureaux offer a way of organising matters in an operational fashion that may prove to be extremely useful in some cases, as for some Contracting Parties this curbs the proliferation of structures.

The following are recommended:

- (a) each Contracting Party may give its Sirene Bureau specific policing and security powers, in line with Title III of the Convention;
- (b) the Contracting Parties shall inform one another of the measures taken at national level for their respective Sirene Bureaux, as well as of any amendments that are made thereafter.

3.2.3. Overlapping roles of Sirene and Interpol

The role of the Schengen Information System is neither to replace nor to copy Interpol. Although there is a certain degree of overlap between tasks, the principles for action and for cooperation between the Contracting Parties differ substantially from those governing the International Criminal Police Organisation.

Consequently, it is necessary to establish the rules for cooperation between the Sirene Bureaux and the NCBs (National Central Bureaux).

The following procedures have been agreed:

(a) Priority of SIS alerts over Interpol alerts

SIS alerts and the exchange of information on these alerts should always have priority over alerts and information exchanged via Interpol. This priority should apply, in particular, if a SIS alert conflicts with an Interpol alert.

(b) Choice of communication channel

Within the territory of the Contracting Parties, alerts in the Schengen Information System take priority over Interpol alerts. Interpol alerts must be restricted to exceptional cases (alerts not provided for in the Convention (for instance, it is not possible to enter alerts for works of art into the SIS) or if not all the necessary information is available for a SIS alert). Parallel alerts in the SIS and via Interpol within the Schengen area are inadmissible. Alerts which are distributed via Interpol channels and which also cover the Schengen area or parts thereof (Interpol diffusion zone 2) should bear the following indication: 'Zone 2 except for the Schengen States'.

(c) Sending information to Third States

The Sirene Bureau of the Contracting Party which issued the alert always decides whether or not to pass information on to third States (authorisation, diffusion means and channel).

In so doing the Sirene Bureau observes the personal data-protection provisions laid down in the Schengen Convention. Use of the Interpol channel will depend on national provisions or procedures.

(d) Targeted search/restricted alerts

A targeted search is a search carried out in a restricted geographical area where there is concrete evidence of the whereabouts of the wanted person or object.

This evidence gives grounds to assume that the request from the judicial authority may be executed immediately on receipt.

Targeted searches in the Schengen area must take place using the A or M form.

An alert for the person or object should be entered in the SIS at the same time as the A or M form is sent, if this has not been done already, so as to make a request for provisional arrest immediately enforceable (Article 64 of the Schengen Convention).

The alert not only complies with the provisions of Article 93 of the Convention but also increases the chances of success should the person or object move unexpectedly from one place to another within the Schengen area.

If a successful result can be achieved by means of a targeted and geographically restricted search, bilateral search requests for provisional arrest in line with the procedure laid down in extradition law may be made without entering an alert in the SIS.

(e) Hit and deletion of an Alert

The Schengen States ensure at national level that the Sirene Bureaux and the NCB inform one another of hits.

The deletion of an alert is undertaken by the authority which issued the alert.

(f) Improvement of cooperation between the Sirene Bureaux and the Interpol NCBs

Each Contracting Party shall take adequate measures to exchange information at national level between the Sirene bureaux and the NCBs.

4. The procedures to be followed

The smooth functioning of the Schengen Information System rests on coordinated action between the various national systems. As a prerequisite for this, common procedures must be defined that are to be followed by all of the Contracting Parties.

Each case requiring intervention has therefore been drawn up and codified to give an accurate description of the tasks to be carried out by the Sirene Bureaux.

- 4.1. The exchange of information prior to an alert
- 4.1.1. Checking whether the national law of the Contracting Parties authorises provisional arrest with a view to extradition (Article 95(2))

The Contracting Party issuing an alert shall check whether the provisional arrest that is to be requested is authorised by the national law of the other Contracting Parties.

The following procedure has been adopted:

- (a) check that all Member States are able to follow up the alert foreseen;
- (b) if there is any doubt, consult the Sirene Bureau concerned and transmit or exchange the information necessary for the check:
- (c) the file provided for by Article 95(2), in the second part of the paragraph, shall be prepared before the alert is entered into the system. It should be checked that all of the information required is contained within the file and that it is presented correctly. The following information is to be transmitted, whereby the details for prosecution or the enforcement of criminal sentences must be given, in principle, as an alternative:
 - 006: Surname: the surname used for the main data in the SIS alert is entered under heading 006.
 - 007: Given name
 - 009: Date of birth

- 010: Place of birth
- 011: Alias: the first alias name is written out in full and the total number of aliases found is indicated. An M Form may be used to send the complete list of alias names.
- 012: Sex
- 013: Nationality: heading 013 'Nationality' must be filled in as completely as possible on the basis of the available information. If there are any doubts as to the information, code '1W', the word 'supposed' should be added to the word 'nationality'.
- 030: Authority issuing the arrest warrant or decision (name and position of the magistrate or public prosecutor or name of the court)
- 031: Reference No of arrest warrant or decision (037)

See also comments below

032: Date of arrest warrant or decision (036)

Requests for criminal prosecution and enforcement can be summarised in an accompanying document.

- 033: Name of requesting authority
- 034: Maximum penalty/maximum penalty foreseen
- 035: Magistrate or court issuing the decision
- 036: Date of decision
- 037: Decision reference number
- 038: Sentence given
- 039: Indication of sentence remaining to be served
- 040: Legal texts applicable
- 041: Legal description of the deeds
- 042: Date/period the offence was committed
- 044: Description of the facts of the case (including their consequences)
- 045: Degree of involvement (principal, accessory, aider, abetter).

Each country may use its own legal terminology to describe the degree of participation (see point 2 of document SCH/OR.SIS-SIRENE (97) 12).

The information given must be in sufficient detail for the other Sirene Bureaux to verify the alert. Nevertheless, only a moderate amount of information should be given in order to avoid unnecessarily overloading the message system.

If the Sirene Bureaux are unable to receive the message because the number of spaces fixed for the relevant form for technical reasons is insufficient, an M form can be sent with supplementary information. The end of the transmission is indicated by the phrase 'End of message' in the last form (heading 044 of Form A or heading 083 of form M).

The Sirene Bureau of the issuing Contracting Party may also provide further information, after consultation and/or at the request of another Contracting Party, if deemed necessary for clarifying an individual's identity. This information shall cover the following in particular:

- the origin of the passport or identity document in the possession of the person sought;
- the passport or identity document's reference number, issuing date, place and authority as well as the expiry date;
- description of the person sought;
- surname and given name of the wanted person's mother and father;
- whether there are records of the person's photo and/ or finger prints;
- last known address.

As far as is possible, this information together with photographs and finger prints shall be available in the Sirene Bureaux, or immediately accessible to them permanently, so that they can transmit these identification elements as soon as possible.

In this highly sensitive area, the common objective should be to minimise the risk of detaining the wrong individual of similar identity to the person on whom an alert has been issued;

- (d) where the alert is admissible by all of the Contracting Parties: the preparations shall be made for it to be entered into the SIS;
- (e) where the alert is not admissible by all of the Contracting Parties:
 - either the issuing Contracting Party abandons the idea of entering the alert,
 - or it persists and asks the Contracting Party (-ies) concerned to submit a request immediately for a flag to be added.

In the event of a flag's being added, the alternative procedure must be implemented by the Contracting Party (-ies) concerned.

4.1.2. Consulting the Contracting Parties for alerts on grounds of State security (Article 99(3))

A Contracting Party issuing an alert for the purposes of discreet surveillance or of a specific check on the grounds of State security is obliged to consult the other Contracting Parties beforehand.

This highly sensitive area requires a specific procedure to safeguard the confidentiality of certain information. To this end, any contact between the services responsible for State security should be kept quite separate from the contact between the Sirene Bureaux.

In this specific case in question, the Sirene Bureaux shall ensure that the consultation procedure functions smoothly and record the results. The information is actually exchanged directly between the specialised services concerned.

The following procedure has been adopted:

- (a) before entering an alert, the security department concerned contacts its Schengen counterparts directly;
- (b) the specialised departments exchange the information they have, after which the security department entering the alert informs its national Sirene Bureau and forwards the results to it. The purpose is mainly to raise any objections that there might be to the planned alert;
- (c) the Sirene Bureau contacted by the security department that is intending to enter an alert shall inform the other Sirene Bureaux. This enables the other bureaux to consult their respective security departments and exercise their rights;
- (d) once the Sirene Bureau of the Contracting Party issuing the alert has established that the formal consultation has been held correctly it then approves the alert's being entered:
- (e) should difficulties arise, the Sirene Bureau concerned shall inform the Contracting Party issuing the alert;
- (f) if the Contracting Party issuing the alert upholds its alert, the requested Contracting Party may request a flag be entered to grant 24 hours to study the matter;

- (g) after this period for further study, at the request of a Contracting Party, a permanent flag may be entered for the alert that suspends the course of action that should otherwise be followed on the grounds of the alert.
- 4.2. Exchange of information when entering an alert
- 4.2.1. Sending a dossier for provisional arrest with a view to extradition (Article 95(2))

This file contains obligatory information as foreseen by the Convention. Furthermore, optional information to assist in processing the matter may also be sent if needed for ascertaining identity.

See comments at point 4.1.1.

A sample form, which is uniform for all of the Contracting Parties, can be found in Annex 5 to this manual.

The following procedure has been adopted:

(a) by the swiftest means available, the Contracting Party issuing the alert shall send the requested Contracting Parties the obligatory information on the case at the same time as entering the alert into the SIS.

If the individual is wanted on the grounds of more than one arrest warrant or verdict, which may serve as a basis for a request for provisional arrest for the purposes of extradition, information on one arrest warrant or one verdict only should initially be sent to the other Sirene Bureaux when entering the alert. The arrest warrant or verdict carrying the highest penalty or the arrest warrant or verdict which takes priority in view of the limitation period should be used.

Information on the other arrest warrants or verdicts should be kept by the Sirene Bureau of the State issuing the alert. In the event of a hit, it should be sent to the Sirene Bureau of the requested State immediately.

If one of the Sirene Bureaux thinks it necessary to add a flag on the basis of the information sent in form A, information on a second arrest warrant or verdict can be

- sent to all Sirene Bureaux so that the alert can be distributed and enforced as widely as possible;
- (b) Any further information required for identification purposes is sent after consultation and/or at the request of another Contracting Party.
- 4.3. The exchange of information for multiple alerts

Pursuant to Article 107, the following general provisions have been adopted:

- (a) only one alert per Contracting Party may be entered into the Schengen Information System for any one individual;
- (b) several Contracting Parties may enter an alert on the same person in the Schengen Information System if the alerts are compatible or if there is no interference between the alerts;
- (c) alerts issued pursuant to Article 95 are compatible with alerts issued pursuant to Articles 97 and 98. Moreover, they may also be considered as compatible with alerts issued pursuant to Article 96. In such cases, the procedures to be followed as set by Article 95 have priority over those set by Article 96;
- (d) alerts issued pursuant to Articles 96 and 99 are not compatible with one another nor with alerts issued pursuant to Articles 95, 97 or 98, without prejudice to Articles 95 and 96 being compatible.

Within the category of alerts issued pursuant to Article 99, 'discreet surveillance' procedures are incompatible with 'specific checks' procedures;

- (e) the order of priority for grounds for alerts is as follows:
 - provisional arrest with a view to extradition (Article 95),
 - non-admission into Schengen States (Article 96),
 - placing under protection (Article 97),
 - discreet surveillance (Article 99),
 - specific checks (Article 99),
 - communicating whereabouts (Articles 97 and 98).

An exception may be made to this order of priority after consultation between the Contracting Parties if essential national interests are at stake;

(f) the Sirene Bureau of the Contracting Party issuing the alert shall keep a record of the requests to enter a new alert rejected after consultation by virtue of the provisions given above, and do so until the alert is deleted.

TABLE OF ALERTS

| | Compatible | Coexisting |
|--|-------------------------------|------------|
| Priority in decreasing order of importance | Grounds for compatible alerts | |
| Article 95 | Articles 95, 97, 98 | Article 96 |
| Article 96 | Article 96 | Article 95 |
| Article 97 | Article 95, 97, 98 | |
| placed under protection | | |
| (table 4, grounds 3, procedure 4 and grounds 4, procedure 5) | | |
| Article 99 | Article 99 | |
| Discreet surveillance | Discreet surveillance | |
| Article 99 | Article 99 | |
| Specific check | Specific check | |
| Articles 97-98 | Articles 95, 97, 98 | |
| Communicate the whereabouts | | |

The specific case of alerts pursuant to Article 96

The provisions of Article 101(2) enable the authorities responsible for issuing visas, for processing visa applications and issuing residence permits to have access to the data pursuant to Article 96.

All alerts pursuant to Article 96 need to be made available to all of the Schengen partners. The objective is not to issue an undesirable alien a residence permit or visa.

This imperative has to be to reconciled with the principles listed above.

The following general provisions have been adopted:

- (a) a Contracting Party should always be able to enter an alert as pursuant to Article 96 so that the competent services do not issue residence permits or visas;
- (b) if there is clash of interests with an alert pursuant to Article 95, each Contracting Party may maintain its alert. The rules on compatibility apply for all the other alerts;

- (c) the procedures to be followed for the alerts shall be applied in the order of priority adopted, in other words, provisional arrest is made first;
- (d) the Contracting Parties shall take the measures necessary at national level to inform their users of this procedure.

The specific case of alerts on vehicles

The following general recommendations have been adopted:

- (a) only one alert per Contracting Party may be entered into the Schengen Information System for any one vehicle;
- (b) several Contracting Parties may enter an alert on the same vehicle in the Schengen Information System if the alerts are compatible;
- (c) alerts on vehicles issued pursuant to Article 99 with 'discreet surveillance' procedures to be followed are incompatible with alerts with 'specific checks' procedures to be followed;
- (d) alerts on vehicles pursuant to Article 99 are incompatible with alerts on vehicles pursuant to Article 100;

(e) the Sirene Bureau of the Contracting Party issuing the alert shall keep a record of the requests for entering a new alert rejected after consultation by virtue of the provisions given above, and do so until the alert is deleted.

TABLE OF COMPATIBLE ALERTS

| Priority by decreasing order of importance | Grounds for alert compatible |
|--|------------------------------|
| Article 99 | Article 99 |
| Discreet surveillance | Discreet surveillance |
| Article 99 | Article 99 |
| Specific check | Specific check |
| Article 100 | Article 100 |

Under exceptional circumstances derogation may be made to the order of priorities indicated above, after consultation between the Contracting Parties, if essential national interests so require.

4.3.1. Checking for multiple alerts on an individual

Multiple alerts will occur only rarely. The main difficulty encountered will be in distinguishing accurately between individuals who have similar characteristics.

To solve this problem, even in cases where alerts are incompatible, cooperation between the Schengen States and policing methods advocate using the procedure for consultation between the Sirene Bureaux.

Each Contracting Party shall set up adequate technical resources to detect possible cases of individuals with identical characteristics before an alert is entered into the SIS.

The identity description elements for concluding that two identities might be identical are detailed in Annex 6 of this manual.

The following procedure has been adopted:

(a) if processing a request for entering a new alert reveals that there is already an individual in the SIS with the

- same mandatory identity description elements (surname, given name, date of birth) a check must be run before the new alert is approved;
- (b) the Sirene Bureau shall contact the requesting department to clarify whether the alert is on the same person or not;
- (c) if the cross-check reveals that the person in question is indeed one and the same, the Sirene Bureau shall apply the procedure for entering multiple alerts as defined in paragraph 4.3.3. If the outcome of the check is that there are in fact two different people, the Sirene Bureau approves the request for entering another alert.

4.3.2. Checking for multiple alerts on a vehicle

The mandatory identity description elements for alerts on a vehicle are:

- either the number plate;
- or the serial number.

However, both numbers may figure in the SIS.

Multiple alerts are checked for by comparing numbers. If two numbers are found to be identical it is assumed that there are multiple alerts on the same vehicle.

Technical difficulties arise with this method of verification in that comparison is not always possible as this depends on the obligatory description elements used.

SIS alerts on vehicles contain the serial number and/or the registration plate number. When entering a new alert, if it is discovered that the same serial number and/or registration plate number already exists in the SIS, it is assumed that there are multiple alerts on the same vehicle.

The Sirene Bureau shall draw the national users' attention to the, certainly limited, number of cases that might cause problems where only one of the numbers has been compared: a positive response, or a 'hit', is taken to mean that there are multiple alerts on one and the same vehicle, but a negative response does not mean that there is no alert on this vehicle. There may be an alert on the vehicle under the number that was not used on the comparative check.

The identity description elements used for concluding that two vehicles are identical are detailed in Annex 6 of this manual.

The procedure to be adopted by the Sirene Bureaux for vehicles is the same as for persons.

4.3.3. Negotiating entering a new alert if it is incompatible with a previous alert

If a request for an alert vies with an alert issued by the same Contracting Party, the national Sirene Bureau should ensure that only one alert is left in the SIS. Each individual State is free to choose the exact procedure to be applied.

If the alert requested is incompatible with an alert that has already been issued by one or several other Contracting Parties, their agreement is required.

The following procedure has been adopted:

- (a) if the alerts are compatible, the Sirene Bureaux do not need to consult; if the alerts do not interfere with one another, the Contracting Party that wishes to enter a new alert shall decide whether consultation ought to be held;
- (b) if the alerts are not compatible, or if there is any doubt, the Sirene Bureaux have to consult so that ultimately only one alert, or one group of alerts that are compatible with one another, is entered into the Schengen Information System;
- (c) if an alert that is incompatible with existing alerts in the SIS is given priority status as the outcome of consultation, the Contracting Parties that entered the other alerts have to withdraw them when the new alert is entered into the SIS;
- (d) any disputes shall be settled by negotiations between the Sirene Bureaux. If agreement cannot be reached on the basis of the list of priorities established, the oldest alert is left in the SIS.

4.4. The exchange of information when adding a flag

The Sirene Bureaux must exchange information so that the Contracting Parties can assess the need for a flag to be added, and thereafter implement this option.

There are three scenarios for adding a flag:

(a) a 'permanent' flag may be added (or deleted) at any moment under the terms of Article 94(4) on alerts pursuant to Articles 95, 97 and 99.

An alternative procedure is foreseen for flags that apply to an alert issued pursuant to Article 95. No alternative procedure is foreseen for alerts pursuant to the other two articles, and the alert does not appear on the screen when the end-user consults the system;

- (b) a flag for 24 hours 'study' time, which may be extended to up to a maximum of seven days, under the provisions of Article 95(3) may be added to alerts pursuant to Article 95. This flag may be converted into a permanent flag. Alternative procedures, as foreseen by Article 95(5), must be followed:
- (c) under the provisions of Article 99(6), a flag for a maximum of 24 hours 'study' may be added to alerts issued pursuant to Article 99. This flag may be converted into a permanent flag. No alternative procedure is foreseen

The Contracting Parties must take the following remarks into account:

- the procedure of adding a flag must be used exceptionally;
- it may take some time between an alert's being entered into the Schengen Information System and a flag's being added. During this time-lapse normal procedures should be followed. This period of time should therefore preferably be kept as short a possible;
- each Contracting Party shall detect the alerts likely to require a flag as swiftly as possible.

4.4.1. Consulting the Contracting Parties with a view to adding a flag

The following procedure has been adopted:

(a) the requested Contracting Party that intends to add a flag to an alert shall inform the Contracting Party that issued the alert.

No consultation is foreseen for a flag added to an alert issued pursuant to Articles 95(3) and 99(6) for the purposes of further study. All Contracting Parties shall be consulted obligatorily for a permanent flag as foreseen under Article 94(4);

(b) once information has been exchanged so as to meet the requirements of each of the Contracting Parties, they may need to amend or even delete either the alert, which is done by the requesting Party, or the request, which is done by the requested Party.

4.4.2. A request for a flag to be added

The following procedure has been adopted:

(a) the requested Contracting Party asks the Contracting Party that issued the alert to add a flag to an alert issued pursuant to Articles 95, 97 or 99.

This request must be made in writing. If the request is made by telephone written confirmation must be given;

- (b) the Contracting Party that issued the alert is obliged to add a flag as soon as possible;
- (c) the same procedure applies for extending a flag added so as to enable further study of an alert issued pursuant to Article 95(3), as well as for withdrawing a temporary or permanent flag;
- (d) in urgent cases, a Contracting Party that issued an alert may ask the requested Contracting Parties to refrain from adding flags for the purposes of further study for alerts issued pursuant to Article 95.

4.4.3. Systematic request for a flag to be added for the State's nationals

The following procedure has been adopted:

- (a) a Contracting Party may ask the Sirene Bureaux of the other Contracting Parties to add a flag as a matter of course to alerts issued on its nationals pursuant to Article 95 if the wanted person is one of its nationals;
- (b) any Contracting Party wishing to take advantage of this option should forward its decision in writing to the Contracting Parties which it would like to cooperate;
- (c) any Contracting Party(ies) to whom this request is addressed shall add a flag for the Contracting Party that has requested one and do so immediately after the alert is issued;
- (d) this procedure shall continue to be binding until another written request is made for it to be cancelled.

4.5. The exchange of information after a hit

4.5.1. Informing the Schengen partners if an alert is matched

The following procedure has been adopted:

(a) a hit after a check has been carried out on an individual, a vehicle or an object on which an alert has been issued

should always be communicated to the Sirene Bureau of the Contracting Party that issued the alert.

On the basis of this information, if deemed necessary the Sirene Bureau of the Contracting Party that issued the alert shall forward any relevant, specific information and the particular measures that should be taken to the Sirene Bureau of the Contracting Party that matched the alert.

When notifying the State which issued the alert of a hit, the Article of the Schengen Convention which applies to the hit should be indicated in heading 090 of form G.

If the hit concerns a person who is registered in the SIS pursuant to Article 95 of the Schengen Convention, the Sirene Bureau of the State in which the hit is obtained should inform the Sirene Bureau of the State issuing the alert by telephone before sending a G form;

- (b) The Sirene Bureaux of Contracting Parties that issued alerts pursuant to Article 96 shall not be informed of any hits as a matter of course. Under exceptional circumstances, the bureaux can be informed by the requested Contracting Party that discovered the alert;
- (c) for each Contracting Party to be able to exercise its rights, the Contracting Parties that had previously indicated that they wanted to issue an alert on the same person or object should preferably be informed of any hits. The Contracting Party that actually issued an alert is responsible for informing these other Contracting Parties;
- (d) through the C.SIS's automatically communicating that an alert has been deleted, it is possible to study whether another alert, which was previously incompatible and which as such was not entered, can in fact now be entered.

4.5.2. Communicating further information

The following procedure has been adopted:

(a) the Sirene Bureaux may transmit further information on alerts issued pursuant to Articles 95, 97, 98 and 100; in so doing they may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance.

The Sirene Bureaux have no powers or particular duties in areas of extradition (1). If an alert issued pursuant to Article 95 is matched, their role simply consists of transmitting further information that the Contracting Parties might require for determining whether extradition procedures should indeed be implemented.

It is not the Sirene Bureaux but the appropriate departments within each Contracting Party that are responsible for transmitting extradition files and other judicial data through the diplomatic channel or other channels;

(b) as far as is possible, the Sirene Bureaux shall communicate medical details on the individuals on whom an alert has been issued pursuant to Article 97 if measures have to be taken for their protection.

The information transmitted is kept only as long as is strictly necessary and is used exclusively for the purposes of medical treatment given to the person concerned;

(c) if operations after an alert is matched so require (such as if an offence is discovered or if there is a threat to law and order, if an object, vehicle or individual needs to be more clearly identified, etc.), the information transmitted as a complement to that stipulated under Title IV of the Schengen Convention, in particular regarding Articles 99 and 100, shall be transmitted by virtue of Articles 39 and 46 of the abovementioned Convention.

The Sirene Bureaux shall send 'further information' as quickly as possible in a P form, in response to a G form when a hit is made on an alert issued on a vehicle pursuant to Article 100 of the Schengen Convention.

NB: (Given that the request is urgent and that it will therefore not be possible to collate all the information immediately, it is agreed that certain headings will be optional rather than obligatory, and that efforts will be made to collate the information relating to the main headings, for example: 041, 042, 043, 162, 164, 165, 166 and 167).

4.6. The exchange of information on aliens not to be granted admission

If an alien who falls under the scenario foreseen in Articles 5 or 25 of the Convention applies for a residence permit or visa the authority issuing the paper must apply specific rules.

Under exceptional circumstances the Schengen partners might need to be informed of the fact that the alert has been matched. Since there are many addressees of alerts issued pursuant to Article 96 in the consular posts and embassies, and given the distances between them, they need not be informed as a matter of course.

4.6.1. Issuing residence permits or visas

The following procedure has been adopted:

- (a) a requested Contracting Party may inform the Contracting Party that issued an alert pursuant to Article 96 of its having been matched. This latter may then inform the other Contracting Parties if it thinks so fit;
- (b) if so requested, whilst respecting national legislation the Sirene Bureaux of the Contracting Parties concerned may assist in transmitting the necessary information to the specialised services responsible for issuing residence permits and visas;
- (c) if the procedure foreseen under Article 25 of the Convention entails deleting an alert issued pursuant to Article 96 the Sirene Bureaux shall, whilst respecting their national legislation, offer their support if so requested.

4.6.2. Refusing admission or expulsion from Schengen territory

The following procedure has been adopted:

- (a) a Contracting Party may ask to be informed of any alerts it issued pursuant to Article 96 that have been matched.
 - Any Contracting Party that wishes to take up this option shall ask the other Contracting Parties in writing;
- (b) a requested Contracting Party may take the initiative and inform the Contracting Party issuing an alert pursuant to Article 96 that the alert has been matched, the alien has not been granted admission or has been expelled from Schengen territory.
- (c) if, on its territory, a Contracting Party intercepts a person for whom an alert has been issued, the Contracting Party issuing the alert may forward the information required to expel (return/deport) a third-country national. Depending on the needs of the requesting Contracting Party and if available to the requested Contracting Party, this information should include the following:
 - the type of decision,
 - the authority issuing the decision,
 - the date of the decision,

- the date of service,
- the date of enforcement.
- the date on which the decision expires or the length of validity.

See point 3(1)(6).

- If a person on whom an alert has been issued is intercepted at the border the procedures set by the issuing Contracting Party have to be followed,
- for the exceptions set out for Articles 5 or 25 of the Convention the requisite consultation must be held between the Contracting Parties concerned via the Sirene Bureaux,
- there might also be an urgent need for complementary information to be exchanged via the Sirene Bureaux in specific cases to identify an individual with certainty.
- 4.7. The exchange of information when the procedure following a hit cannot be executed

4.7.1. Informing the alerting Contracting Party that the procedures cannot be followed

The following procedure has been adopted:

- (a) the requested Contracting Party shall inform the Contracting Party that issued the alert straight away, and do so via its Sirene Bureau, of the fact that it is not able to follow procedures, and give the reasons;
- (b) the Contracting Parties concerned may then agree on what procedure to follow in keeping with their own national legislation and with the provisions of the Convention.
- 4.8. The exchange of information if the objective of the alert is changed

The consent of the Contracting Party that issued the alert is required for this procedure that is used only under exceptional circumstances. The issuing Contracting Party should be able to appraise the importance and relevance of the request.

The ends for which the data are to be used must come under one of the alert categories foreseen in Articles 95 to 100 of the Convention.

On no account should this data be used for other ends than those foreseen by the Convention.

4.8.1. Informing the alerting Contracting Party that the objective has been changed

The following procedure has been adopted:

- (a) through its Sirene Bureau, the requested Contracting Party shall explain to the Contracting Party that issued the alert the grounds for its asking for the original objective to be changed;
- (b) as soon as possible, the issuing Contracting Party shall study whether this wish can be met and advise the requested Contracting Party through its Sirene Bureau of its decision.

If need be, the Contracting Party that issued the alert can grant authorisation subject to certain conditions on how the data are to be used.

4.8.2. Procedures for changing the original objective

The following procedure has been adopted:

- (a) once the Contracting Party that issued the alert has agreed, the requested Contracting Party shall use the data for the ends it sought and obtained authorisation. It shall take account of any conditions set.
- 4.9. The exchange of information in the case of inaccurate or inadmissible data

4.9.1. Informing the alerting Contracting Party that data is inaccurate or inadmissible

The following procedure has been adopted:

- the Contracting Party that establishes that data contain an error shall advise the issuing Contracting Party thereof via its Sirene Bureau;
- information shall be exchanged so as to reach an agreement on how this data should be corrected or deleted;

- (c) form J may be used when inaccurate or inadmissible data is detected as well as to transmit the reply from the Sirene Bureaux issuing the alert;
- (d) the additional information required to establish identity should be sent on agreement with and/or at the request of another Contracting Party.

4.9.2. Rectification procedures

The following procedure has been adopted:

- (a) if the Contracting Parties are in agreement, the issuing Contracting Party shall follow its national procedures for correcting the error;
- (b) if there is no agreement, the Sirene Bureau of the Contracting Party that established the error shall advise the authority responsible within its own country to referral of the matter to the Joint Supervisory Authority.
- 4.10. The exchange of information regarding the right to access or rectify data

4.10.1. Informing the national authorities of a request to access or rectify data

The following procedure has been adopted:

- (a) each Sirene Bureau must apply its national legislation on the right to access to the data. Depending on the circumstances of the case, the Sirene Bureaux shall either forward the national authorities responsible any requests they receive for access or for rectifying data, or they shall adjudicate upon these requests within the limits of their remit:
- (b) If the national authorities responsible so ask, the Sirene Bureaux of the Contracting Parties concerned shall forward information on exercising this right to access.

4.10.2. Information on requests for access for alerts issued by other Contracting Parties

As far as is possible, information on alerts entered into the SIS by another Contracting Party shall be exchanged via the national Sirene Bureaux.

The following procedure has been adopted:

- (a) the request for access shall be forwarded to the Contracting Party that issued the alert as soon as possible, so that it can take a position on the question;
- (b) the issuing Contracting Party shall inform the Contracting Party that received the request of its position.
 - It shall take account of any legal deadlines set for processing the request;
- (c) if the Contracting Party that issued the alert sends its position to the Sirene Bureau of the Contracting Party that received the request for access, the Sirene Bureau shall ensure that the position is forwarded to the authority responsible for adjudication on the request as soon as possible.

4.10.3. Information on access and rectification procedures

The following procedure has been adopted:

(a) the Sirene Bureaux shall keep one another informed of any national legislation adopted on access and rectification procedures for personal data, as well as of any amendments made thereafter.

5. The tasks to be performed per alert category

Several problems have to be addressed by the Sirene Bureaux when an alert is entered into the SIS. They must ensure that that the provisions set out in the Schengen Convention are respected and guarantee the technical status of the data.

The sequence of tasks to be performed for each category of alerts must be followed scrupulously so as to guarantee that the information distributed through the SIS is reliable.

The moment a hit is made, the main duty is to notify straight away that the alert has been matched. Should circumstances so require, any further information that might be needed for action to be taken shall be exchanged between the Contracting Parties concerned.

5.1. Creating an alert

5.1.1. The tasks common to all categories

The following tasks must be carried out before any action is taken which relates specifically to one category of alerts:

- (a) check for multiple alerts:
 - at national level there may only be one alert in the SIS per country on any one individual (or vehicle).
 In the event of their being more than one, national procedures must be followed to ensure that only one alert is left in the SIS,
 - within Schengen, there may be several compatible alerts on any one individual (or vehicle);
- (b) if there is more than one alert on any one individual (or vehicle) check that they are compatible:
 - if they are not compatible, negotiate entering only one alert (on any one individual or vehicle). In the event of failure to come to an agreement: the procedure is terminated here,
 - if the multiple alerts are compatible, or if it is agreed that the new alert should be given priority, continue with the procedure.

Please note: The contracting Party issuing the alert should keep a copy of requests for entering an alert that are rejected so that it can communicate all the hits of which it has been informed.

The Contracting Party that was not able to enter its alert shall take the necessary technical measures to review its request if it is notified automatically that the alert previously blocking its request has been deleted.

5.1.2. Measures to be taken for each individual category of alert

5.1.2.1. Alerts pursuant to Article 95

- (a) Check that the national legislation of the Contracting Parties authorises provisional arrest for the purpose of extradition.
- (b) Check whether there is a file on obligatory complementary information.
- (c) Enter the alert into the SIS and at the same time send the file to the other Sirene Bureaux.
- (d) At the request of another Contracting Party add a flag.

5.1.2.2. Alerts pursuant to Article 96

(a) Enter the alert into the SIS.

- 5.1.2.3. Alerts pursuant to Article 97
- (a) Enter the alert into the SIS.
- (b) At the request of a Contracting Party add a flag.
- 5.1.2.4. Alerts pursuant to Article 98
- (a) Enter the alert into the SIS.
- 5.1.2.5. Alerts pursuant to Article 99(2)
- (a) Enter the alert into the SIS.
- (b) At the request of another Contracting Party add a flag.
- 5.1.2.6. Alerts pursuant to Article 99(3)
- (a) Check with the national security services that the security services in the other Contracting Parties have been informed.
- (b) Inform the Sirene Bureaux in the other Contracting Parties of the new alert and ensure that cooperation and consultation take place correctly.
- (c) Enter the alert into the SIS.
- (d) At the request of a Contracting Party add a flag.
- 5.1.2.7. Alerts pursuant to Article 100
- (a) For vehicles only: check for multiple alerts, and if there is more than one alert, check that the alerts are compatible.
- (b) Enter the alert into the SIS.
- (c) An alert for a vehicle should be issued by the State in which the first report was made.
- 5.2. Amending an alert

5.2.1. Entering an alias

(a) Check that the alias that is due to be entered is not a multiple alert. If there is any doubt or if there is a multiple alert, follow procedures foreseen for this.

The party that entered the original alert is responsible for adding any aliases. If a third country discovers the alias it should pass the matter on to the party that originally entered the alert, unless the third country itself issues an alert on the alias.

- (b) Inform the other Contracting Parties of aliases regarding an alert issued pursuant to Articles 95 or 99(3). Whenever needed, the Sirene Bureaux shall transmit this information to their national authorities responsible for each category of alert.
- (c) Enter the alert into the SIS.

5.2.2. Changing the grounds or procedures for an alert

This procedure shall be applied regardless of a hit.

- (a) Delete the alert that is to be placed in another category
- (b) Recommence the entire procedure for entering an alert in the new category.

5.3. Deleting an alert

5.3.1. Deleting after a hit

(a) Inform the Contracting Parties who had been unable to enter their alert that a hit has been made and that the alert has been deleted.

5.3.2. Deleting when the conditions for maintaining the alert cease to be met

Excluding the cases after a hit, an alert may be deleted either directly by the C.SIS (once the expiry date is passed) or indirectly by the service that entered the alert in the SIS (once the conditions for the alert's being maintained no longer apply).

In both instances the C.SIS delete message should be processed automatically by the N.SIS so that an alert kept pending can be entered in its place.

- (a) The Sirene Bureau is notified automatically by a message from its N.SIS that an alert put on hold can be entered.
- (b) The Sirene Bureau shall apply the entire procedure for entering an alert in the appropriate alert category.