►**B** ►**M2** **Revised Sirene Manual** [1] ◄ ◄

(OJ C 38, 17.2.2003, p. 1)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Commission Decision 2006/757/EC of 22 September 2006	L 317	1	16.11.2006
►**M2**	Commission Decision 2006/758/EC of 22 September 2006	L 317	41	16.11.2006

[1] This text is identical to the text in the Annex to Decision 2006/757/EC (see page 1 of this Official Journal).

▼B
▼M2

Revised Sirene Manual [1]

CONTENTS

Introduction . . . . .

1. THE SCHENGEN INFORMATION SYSTEM (SIS) AND NATIONAL SIRENES . . . . .

1.1. Legal basis (Article 92(4) Schengen Convention) . . . . .

1.2. The Sirene bureau . . . . .

1.3. Sirene Manual . . . . .

1.4. Standards . . . . .

1.4.1. Availability . . . . .

1.4.2. Continuity . . . . .

1.4.3. Security . . . . .

1.4.4. Accessibility . . . . .

1.4.5. Communications . . . . .

1.4.6. Transliteration rules . . . . .

1.4.7. Data quality . . . . .

1.4.8. Structures . . . . .

1.4.9. Archiving . . . . .

1.5. Staff . . . . .

1.5.1. Knowledge . . . . .

1.5.2. Training . . . . .

1.5.3. Exchange of staff . . . . .

1.6. Technical infrastructure . . . . .

1.6.1. Automatic introduction of data . . . . .

1.6.2. Automatic deletion of data . . . . .

1.6.3. Data exchange between Sirene bureaux . . . . .

1.6.4. Data quality SIS . . . . .

2. GENERAL PROCEDURES . . . . .

2.1. Multiple alerts (Article 107) . . . . .

2.1.1. The exchange of information for multiple alerts . . . . .

2.1.2. Checking for multiple alerts on a person . . . . .

2.1.3. Negotiating entering a new alert if it is incompatible with an

[1] This text is identical to the text in the Annex to Decision 2006/757/EC (see page 1 of this Official Journal).

▼M2

existing alert (E form) . . . . . .

2.2. The exchange of information after a hit . . . . . .

2.2.1. Communicating further information . . . . . .

2.3. When the procedures following a hit cannot be followed (Article 104(3) . . . . . .

2.4. If the original purpose of the alert is altered (Article 102(3) .

2.4.1. Procedures for changing the original purpose . . . . . .

2.5. Data found to be legally or factually inaccurate (Article 106)

2.5.1. Rectification procedures . . . . . .

2.6. The right to access and rectify data (Articles 109 and 110) . .

2.6.1. The exchange of information regarding the right to access or rectify data . . . . . .

2.6.2. Information on requests for access to alerts issued by other Member States . . . . . .

2.6.3. Information on access and rectification procedures . . . . . .

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

2.8. Misused identity . . . . . .

2.9. Sirpit (Sirene Picture Transfer) . . . . . .

2.9.1. Development and background of Sirpit (Sirene Picture Transfer) . . . . . .

2.9.2. Further use of the data exchanged, including archiving . . . .

2.9.3. Technical requirements . . . . . .

2.9.4. The national identification service . . . . . .

2.9.5. Use of the Sirene **L form** . . . . . .

2.9.6. Sirpit procedure . . . . . .

2.9.6.1. The discovering Sirene bureau makes the comparison . . . . .

2.9.6.2. The providing Sirene bureau makes the comparison . . . . . .

2.9.6.3. Input screen . . . . . .

2.10. Police cooperation (Articles 39 to 46) . . . . . .

2.10.1. Specific powers in policing and security matters. Title III. (Articles 39 and 46) . . . . . .

2.11. Overlapping roles of Sirene and Interpol . . . . . .

2.11.1. Priority of SIS alerts over Interpol alerts . . . . . .

2.11.2. Choice of communication channel . . . . . .

2.11.3. Use and distribution of Interpol in Schengen States . . . . . .

▼M2

2.11.4. Sending information to third States . . . . . .

2.11.5. Hit and deletion of an alert . . . . . .

2.11.6. Improvement of cooperation between the Sirene bureaux and the Interpol NCBs . . . . . .

2.12. Cooperation with Europol and Eurojust . . . . . .

2.13. Special types of search . . . . . .

2.13.1. Geographically targeted search . . . . . .

2.13.2. Search with participation of special police units of targeted search . . . . . .

2.14. Adding a flag . . . . . .

2.14.1. The exchange of information when adding a flag . . . . . .

2.14.2. Consulting the Member States with a view to adding a flag .

2.14.3. A request for a flag to be added . . . . . .

2.14.4. Systematic request for a flag to be added to a Member State's nationals . . . . . .

3. ALERTS PURSUANT TO ARTICLE 95 . . . . . .

3.1. Member State checks prior to issuing the alert. . . . . .

3.2. Checking whether the national law of the Member States authorises arrest with a view to surrender or extradition . . . .

3.3. Multiple alerts . . . . . .

3.3.1. Check for multiple alerts (Article 107) . . . . . .

3.3.2. Exchange of information . . . . . .

3.3.3. Entering an alias . . . . . .

3.4. Supplementary information to be sent to Member States . . .

3.4.1. Supplementary information to be sent with regards to an EAW

3.4.2. Supplementary information to be sent with regards to provisional arrest . . . . . .

3.4.3. Further information to establish a person's identity . . . . . .

3.4.4. Sending the **A** and **M forms** . . . . . .

3.5. At the request of another Member State to add a flag . . . . .

3.5.1. The exchange of information when adding a flag . . . . . .

3.5.2. Consulting the Member States with a view to adding a flag .

3.5.3. A request for a flag to be added . . . . . .

3.5.4. Systematic request for a flag to be added to a Member State's nationals . . . . . .

3.6. Action by Sirene bureaux upon receipt of an Article 95 alert

▼M2

3.7. The exchange of information after a hit . . . . . .

3.7.1. Informing the Member States if an alert is matched . . . . . .

3.7.2. Communicating further information . . . . . .

3.7.3. Following a hit . . . . . .

3.8. Deletion of an alert . . . . . .

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

3.9. Misused identity . . . . . .

3.9.1. Gathering and communicating information on the person whose identity is misused . . . . . .

3.9.2. Communicating information on a person whose identity is misused . . . . . .

4. ALERTS PURSUANT TO ARTICLE 96 . . . . . .

4.1. Introduction . . . . . .

4.2. Alerts pursuant to Article 96 . . . . . .

4.3. Entering an alias . . . . . .

4.4. Misused identity . . . . . .

4.4.1. Gathering and communicating information on a person whose identity is misused . . . . . .

4.5. Issuing residence permits or visas . . . . . .

4.6. Refusing admission or expulsion from Schengen territory . . .

4.7. The exchange of information on third country nationals not to be granted admission . . . . . .

4.8. Informing the Schengen Member States if an alert is matched

5. ALERTS PURSUANT TO ARTICLE 97 . . . . . .

5.1. Alerts pursuant to Article 97 . . . . . .

5.2. Adding a flag . . . . . .

5.2.1. The exchange of information when adding a flag . . . . . .

5.2.2. Consulting the Member States with a view to adding a flag .

5.2.3. A request for a flag to be added . . . . . .

5.3. After a hit . . . . . .

5.3.1. Communicating further information . . . . . .

6. ALERTS PURSUANT TO ARTICLE 98 . . . . . .

6.1. Alerts pursuant to Article 98 . . . . . .

6.2. After a hit . . . . . .

6.2.1. Communicating further information . . . . . .

▼**M2**

7. ALERTS PURSUANT TO ARTICLE 99 . . . . . .

7.1. Alerts pursuant to Article 99(2) . . . . . .

7.2. Entering an alias . . . . . .

7.3. Consulting the Member States prior to alerts on grounds of State security . . . . . .

7.4. Adding a flag . . . . . .

7.4.1. The exchange of information when adding a flag . . . . . .

7.4.2. Consulting the Member States with a view to adding a flag .

7.4.3. A request for a flag to be added . . . . . .

7.5. Communicating further information following a hit . . . . . .

8. ALERTS PURSUANT TO ARTICLE 100 . . . . . .

8.1. Vehicle alerts pursuant to Article 100 . . . . . .

8.1.1. Checking for multiple alerts on a vehicle. . . . . .

8.1.2. The specific case of alerts on vehicles. . . . . .

8.2. Communicating further information following a hit . . . . . .

9. STATISTICS . . . . . .

▼M2

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 Member States 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 to the Agreement in November 1988, lays down the broad technical principles for setting up the Schengen Information System (SIS).

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: **S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntries.

This is 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 founding countries signed the Convention implementing the Schengen Agreement ([2]) 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 that are binding on all of the Member States. Norway and Iceland also concluded a Cooperation Agreement with the Member States on 19 December 1996.

The Schengen *acquis* — Convention was incorporated into the legal framework of the European Union by means of protocols attached to the Treaty of Amsterdam in 1999. A Council Decision was adopted on 12 May 1999 determining in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen *acquis.*

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

The **S**chengen **I**nformation **S**ystem (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.

([2]) OJ L 239, 22.9.2000, p. 19.

▼M2

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).

It should, nonetheless, be possible for the Member States 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 multi-lateral basis.

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

This is the technical operational service that will be used and will be responsible for transmitting all supplementary information requests at the National Entries.

The following principle has been adopted by the Member States:

A 'national Sirene bureau' shall be set up by each of the Member States 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 jointly by all Member States so as to have common rules. The arrangements are recorded in this 'Sirene Manual'.

1. THE SCHENGEN INFORMATION SYSTEM (SIS) AND NATIONAL SIRENES

The SIS, set up pursuant to the provisions of Title IV of the Convention of 1990, implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (Schengen Convention) ([3]) constitutes an essential tool for the application of the provisions of the Schengen *acquis* as integrated into the framework of the European Union.

1.1. Legal basis (Article 92(4) Schengen Convention) ([4])

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

1.2. The Sirene bureau

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 is necessary for the Schengen Member States to be able to exchange supplementary information required for implementing certain provisions laid in the convention, and for the SIS to function properly, either on a bilateral or multilateral basis.

([3]) See footnote 2.

([4]) Unless otherwise stipulated all articles referred to are to be understood as articles of the Convention of 1990, implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (Schengen Convention).
Article 92(4) took effect according to Article 1(1) of Council Decision 2005/451/JHA (OJ L 158, 21.6.2005, p. 26) and Article 2(1) of Decision 2005/211/JHA (OJ L 68, 15.3.2005, p. 44).

▼M2

To meet the operating constraints set out in the convention, every Schengen Member State has to establish a central authority as a single contact point for exchanging supplementary information related to SIS data. This contact point, which is referred to as Sirene bureau, has to be fully operational on a 24/7 basis.

1.3. **Sirene Manual**

The Sirene Manual is a set of instructions for Sirene bureaux, which describes in detail the rules and procedures governing the bilateral or multilateral exchange of the supplementary information referred to in paragraph 1.2

1.4. **Standards**

The fundamental standards that underpin the cooperation via Sirene are the following:

1.4.1. *Availability*

A national Sirene bureau shall be set up by each of the Member States to serve as a single contact point for the Member States applying the Schengen Convention. It shall be fully operational 24 hours a day. Availability for technical analysis, support and solutions shall also be provided 24 hours a day.

1.4.2. *Continuity*

Each Sirene bureau shall build an internal structure, which guarantees the continuity of management, staff and technical infrastructure.

The heads of each Sirene bureau shall meet at least twice a year to assess the quality of the cooperation between their services, to adopt necessary technical or organisational measures in the event of any difficulties and to adjust procedures where required.

1.4.3. *Security*

Security on premises

Physical and organisational security features are necessary to protect the Sirene bureau premises. The specific measures will be determined by and be dependant on, the results of threat assessments that will be carried out by each Schengen State. Recommendations and best practices laid down in Volume 2 of the EU Schengen Catalogue: Schengen Information System, Sirene, should be reflected in practice, as should Council Decision 2001/264/EC ([5]).

The specific features may differ as they will have to answer to threats in the immediate surroundings and exact location of the Sirene bureau. They may include:

— external windows fitted with security glass,

— secured and closed doors,

— brick/concrete walls enclosing of the Sirene bureau,

— intrusion alarms, including logging of entries, exits and any unusual event,

— security guards on site or rapidly available,

— fire extinction system and/or direct link to fire brigade,

— dedicated premises to avoid staff who are not involved in international police cooperation measures, or who do not

([5]) OJ L 101, 11.4.2001, p . 1.

▼M2

have requisite access to documents from having to enter or to pass the Sirene bureau offices, and/or

— sufficient back-up power supply.

Security on the system

The principles underlying the security of the system are set out in Article 118 of the Schengen Convention.

Ideally, the Sirene bureau system should have a back up computer and data base system at a secondary site in case of a serious emergency at the Sirene bureau.

1.4.4. *Accessibility*

In order to fulfil the requirement to provide supplementary information, the Sirene staff shall have direct or indirect access to all relevant national information and expert advice.

1.4.5. *Communications*

Operational

The specific channel to use for Sirene communications shall be jointly decided by the Schengen Member States. Only if this channel is not available, another, and given the circumstances the most appropriate, means of communication shall be determined on a case by case basis, according to technical possibilities and the security and quality requirements that the communication has to meet.

Written messages are divided into two categories: free text and standard forms. The latter must respect the instructions set out in Annex 5. The B ([6]), C ([7]) and D ([8]) forms shall not be used any longer and are removed from Annex 5.

In order to achieve utmost efficiency in bilateral communication between Sirene staff, a language familiar to both parties shall be used.

The Sirene bureau shall answer all requests for information made by the other Member States via their Sirene bureaux as soon as possible. In any event a response shall be given within 12 hours.

Priorities in daily work shall be based on the type of the alert and the importance of the case.

Non-operational

The Sirene bureau should use the dedicated SIS-NET e-mail address for the exchange of non-operational information.

1.4.6. *Transliteration rules*

Transliteration rules, which can be found in Annex 2, have to be followed.

1.4.7. *Data quality*

It is the responsibility of each Sirene bureau to perform the role of data quality assurance coordinator for the information that is introduced in the SIS. To this end Sirene bureaux shall have the necessary national competence to perform this role, for which it is responsible pursuant to Article 92(4) and Article 108. It is therefore necessary to have some form of national data quality audit, including a review of the rate of alerts/hits and of data content.

([6]) Information further to an alert regarding State security.
([7]) Checking for a double alert on the same person.
([8]) Checking for a double alert on the same vehicle.

▼M2

National standards for training of end-users on data quality principles and practice should be established.

1.4.8. *Structures*

All national agencies, including Sirene bureaux, responsible for international police cooperation must be organised in a structured fashion so as to prevent conflicts of powers with other national bodies carrying out similar functions and duplication of work.

1.4.9. *Archiving*

(a) Each Member State shall determine the provisions for storing information.

(b) The Sirene bureau of the Member State issuing the alert is obliged to keep all of the information on its own alerts available to the other Member States.

(c) The archives of each Sirene bureau should allow swift access to the relevant information to meet the very short deadlines for transmitting information.

(d) The files and other messages sent by the other Member States shall be stored according to national data and privacy protection legislation in the recipient Member State. The provisions of Title VI of the Schengen Convention and the Directive 95/46/EC of the European Parliament and of the Council [9] shall also apply. As far as is possible, these additional pieces of information will not be kept by the Sirene bureaux once the corresponding alert is deleted

(e) Misused identity: Information on misused identity should be deleted after the deletion of the relevant alert.

1.5. **Staff**

1.5.1. *Knowledge*

Sirene bureau staff shall have the linguistic skills covering as wide a range of languages as possible and on-duty staff shall able to communicate with all Sirene bureaux.

They shall have the necessary knowledge on:

— national and international legal aspects,

— their national law enforcement agencies, and

— national and European judiciary and immigration administration systems.

They need to have the authority to deal independently with any incoming case.

In case of special requests or (legal) expert advice, they should have the possibility to call upon the assistance of their superiors and/or experts.

Operators on duty outside office hours shall have the same competence, knowledge and authority and have the possibility to refer to experts available on-call.

Legal expertise to cover both normal and exceptional cases is required. Depending on the cases, this can be provided by any personnel with the necessary legal background or experts from the judicial authorities

The national responsible recruiting authorities have to take all the above skills and knowledge into consideration when

[9] OJ L 281, 23.11.1995, p. 31.

▼M2

recruiting new staff and, consequently, organise in-service training courses or sessions both at national and international level.

A high level of experience of staff leads to a workforce able to function on their own initiative and thereby able to handle cases efficiently. Therefore a low turnover of personnel is propitious, which requires the unambiguous support of management to enable this devolved responsibility.

1.5.2. *Training*

National level

At national level, sufficient training shall ensure that staff meet the required standards laid down in this manual.

It is recommended that Sirene bureaux be involved in the training of all authorities entering alerts, stressing data quality and maximisation of the use of the SIS.

International level

Common training courses shall be organised at least once a year, to enhance cooperation between Sirene bureaux by allowing staff to meet colleagues from other Sirene bureaux, share information on national working methods and create a consistent and equivalent level of knowledge. It will furthermore make staff aware of the importance of their work and the need for mutual solidarity in view of the common security of Member States.

1.5.3. *Exchange of staff*

Sirene bureaux may also consider the possibility of setting up staff exchanges with other Sirene bureaux. These exchanges are intended to help improve staff knowledge of working methods, to show how other Sirene bureaux are organised and to establish personal contacts with colleagues in other Member States.

1.6. **Technical infrastructure**

In general, the technical resources are the established methods by means of which information is communicated between the Sirene bureaux.

Each Sirene bureau shall have a computerised management system, which allows a great deal of automation in the management of the daily workflow

1.6.1. *Automatic introduction of data*

Automatic transfer to N.SIS of the national alerts that fulfil the criteria for introduction into the SIS shall be the preferred way to introduce SIS alerts. This automatic transfer, including data quality checks, should also be transparent and not require an additional action from the authority entering the alert

1.6.2. *Automatic deletion of data*

Where the national system enables the automatic transfer of national alerts to SIS, as set out in the previous paragraph, the deletion of a SIS-related alert in the national database should also lead to an automatic deletion of its SIS equivalent.

Since multiple alerts are not allowed, it is recommended that wherever possible and necessary, second and subsequent alerts on the same person are kept available at national level so that they can be introduced when the first alert on this person expires.

▼M2

1.6.3. *Data exchange between Sirene bureaux*

The instructions laid down for data exchange between Sirene bureaux shall be respected ([10]).

1.6.4. *Data quality SIS*

In order to allow each Sirene bureau to perform its role of data quality assurance coordinator (see paragraph 1.5 above), the necessary IT support should be available.

2. **GENERAL PROCEDURES**

The procedures described below are applicable to almost all of Articles 95 to 100, and the procedures specific for each article can be found in the description of the following article:

2.1. **Multiple alerts (Article 107)**

Several alerts issued by different countries for the same subjects may sometimes occur. It is essential that this does not cause confusion to end-users, and that they are clear as to the measures which must be taken when seeking to enter an alert. Various procedures shall therefore be established for detecting multiple alerts and a priority mechanism shall also be established for entering them into the SIS.

This calls for:

— checks before entering an alert, in order to determine whether the subject is already in the SIS,

— consultation with the other Member States, when the entry of an alert will cause multiple alerts that are incompatible.

2.1.1. *The exchange of information for multiple alerts*

Only one alert per Member State may be entered into the SIS for any one individual;

Several Member States may enter an alert on the same person if the alerts are compatible or may coexist;

Article 95 alerts are compatible with Article 97 and 98 alerts. They may also co-exist with Article 96 alerts, although in such cases, the Article 95 procedures have priority over those set for Article 96.

(a) Article 96 and 99 alerts are not compatible with each other or with Articles 95, 97 or 98 alerts, without prejudice to Articles 95 and 96 alerts being coexistent.

Within Article 99, alerts issued for ‘discreet surveillance’ are incompatible with those for ‘specific checks’;

(b) The order of priority for alerts is as follows:

— arrest with a view to surrender or extradition (Article 95),

— non-admission into Schengen States (Article 96),

— placing under protection (Article 97),

— discreet surveillance (Article 99),

— specific checks (Article 99), and

— communicating whereabouts (Articles 97 and 98).

Departures from this order of priority may be made after consultation between the Member States if essential national interests are at stake.

([10]) Document SN 1503/1/00, version No 5.1.

▼M2

Table of alerts

Order of importance	Article 95	Article 96	Article 97 protection	Article 99 (DS) person	Article 99 (SC) person	Article 97 whereabouts	Article 98	Article 99 (DS) vehicle	Article 99 (SC) vehicle	Article 100
Article 95	yes	may co-exist	yes	no	no	yes	yes	X	X	X
Article 96	may co-exist	yes	no	no	no	no	no	X	X	X
Article 97 protection	yes	no	yes	no	no	yes	yes	X	X	X
Article 99 disc.surv. Person	no	no	no	yes	no	no	no	X	X	X
Article 99 sp. check person	no	no	no	no	yes	no	no	X	X	X
Article 97 where-abouts	yes	no	yes	no	no	yes	yes	X	X	X
Article 98	yes	no	yes	no	no	yes	yes	X	X	X
Article 99 (DS) Vehicle	X	X	X	X	X	X	X	Yes	no	no
Article 99 (SC) Vehicle	X	X	X	X	X	X	X	No	yes	no
Article 100	X	X	X	no	no	X	X	No	no	yes

(X means not applicable)

2.1.2. *Checking for multiple alerts on a person*

To avoid entering incompatible multiple alerts, care must be taken to distinguish accurately between individuals who have similar characteristics. Consultation and cooperation between the Sirene bureaux is therefore essential, and each Member State shall establish appropriate technical procedures to detect such cases before an entry is made.

The elements used for establishing whether two identities may 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 a person 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 national issuing Sirene bureau to clarify whether the alert relates to the same person (L form); and

(c) if the check reveals that the details are identical and could relate to the same person, the Sirene bureau shall apply the procedure for entering multiple alerts. If the outcome of the

▼M2

check is that the details relate to two different people, the Sirene bureau shall approve the request for entering the new alert.

2.1.3. *Negotiating entering a new alert if it is incompatible with an existing alert (E form)*

If a request for an alert conflicts with an alert issued by the same Member State, the national Sirene bureau shall ensure that only one alert exists in the SIS. Each Member State may choose the procedure to be applied.

If the alert requested is incompatible with an alert already issued by one or several other Member States, 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 are independent of each other, the Member State that wishes to enter a new alert shall decide whether to consult;

(b) if the alerts are not compatible, or if there is any doubt as to their compatibility, the Sirene bureaux shall consult one another so that ultimately only one alert is entered;

(c) if an alert that is incompatible with existing alerts is given priority as the outcome of consultation, the Member States that entered the other alerts shall withdraw them when the new alert is entered; 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;

(d) if an alert is deleted, Member States who were not able to enter an alert are informed by the C.SIS. The Sirene bureau then should be notified automatically by a message from N.SIS that an alert put on hold can be entered. The Sirene bureau shall apply the entire procedure for entering an alert in the appropriate alert category.

2.2. **The exchange of information after a hit**

When an end-user conducts a search of the SIS and finds that an alert exists which matches the details entered, this is called a ‘hit’.

The end-user may require the Sirene bureau to supply supplementary information in order to allow effective implementation of the procedures laid down in SIS tables 4, 10 or 16 as set out in Annex 4.

Unless stated otherwise, the issuing Member State must be informed of the hit and its outcome.

The following procedure has been adopted:

(a) a hit on an individual or an object on which an alert has been issued should usually be communicated to the Sirene bureau of the issuing Member State.

If necessary the Sirene bureau of the issuing Member State shall then send any relevant, specific information and the particular measures should be taken by the Sirene bureau of the Member State that matched the alert.

When notifying the Party 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 the G form.

If the hit concerns a person who is the subject of an Article 95 alert, the Sirene bureau of the Member State

▼M2

that matched the alert should inform the Sirene bureau of the issuing Member State of the hit by telephone after sending a G Form;

(b) the Sirene bureaux of Member States that have issued alerts under Article 96 shall not necessarily be informed of any hits as a matter of course, but may be informed in exceptional circumstances. A G form can be sent if for example supplementary information is required;

(c) C.SIS automatically communicates the deletion of an alert to all Member States.

2.2.1. *Communicating further information*

The following procedure has been adopted:

(a) the Sirene bureaux may transmit further information on Article 95 to Article 100 alerts, and in doing so may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance;

(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 Art. 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 after an alert is matched operations so require (e.g. 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. Appropriate measures have to be taken by every Member State in order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46;

(d) 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.

2.3. **When the procedures following a hit cannot be followed (Article 104(3))**

Under Article 104(3) a Member State, which is unable to follow the procedure, required by an alert shall immediately notify the issuing Member State by using an **H form.**

If when following a hit, normal procedures cannot be executed, the exchange of data should take place according to the following rules:

(a) the discovering Member State shall immediately inform the Member State that issued the alert via its Sirene bureau, that it is not able to follow procedures, and give the reasons by using an **H form**;

(b) the Member States concerned may then agree on what procedure to follow in keeping with their own national legislation and with the provisions of the Convention.

2.4. **If the original purpose of the alert is altered (Article 102(3))**

Under Article 102(3), the data may be used for a purpose other than that for which the alert was entered, but only following a hit in order to prevent an imminent serious threat to public

▼M2

order and safety, for serious reasons of State security or for the purposes of preventing a serious criminal offence.

The purpose of the alert may only be altered if prior authorisation has been obtained from the issuing Member State.

If the purpose of the alert is changed, the exchange of information should take place according to the following rules:

(a) through its Sirene bureau, the discovering Member State shall explain to the Member State that issued the alert the grounds for its asking for the original objective to be changed (**I form**);

(b) as soon as possible, the issuing Member State shall study whether this wish can be met and advise the discovering Member State, through its Sirene bureau, of its decision;

(c) if need be, the Member State that issued the alert can grant authorisation subject to certain conditions on how the data is to be used.

2.4.1. *Procedures for changing the original purpose*

The following procedure has been adopted:

Once the Member State that issued the alert has agreed, the discovering Member State shall use the data for the reason it sought and obtained authorisation. It shall take account of any conditions set.

2.5. **Data found to be legally or factually inaccurate (Article 106)**

Paragraphs 2 and 3 of Article 106 provide for legal or factual errors to be rectified.

If data is found to be legally or factually incorrect or inadmissible, then the exchange of information will take place according to the following rule:

The Member State which establishes that data contains an error shall advise the issuing Member State via its Sirene bureau by using the J form.

2.5.1. *Rectification procedures*

The following procedure has been adopted:

(a) if the Member States are in agreement, the issuing Member State shall follow its national procedures for correcting the error.

(b) if there is no agreement, the Sirene bureau of the Member State that established the error shall advise the authority responsible within its own country to referral of the matter to the Joint Supervisory Authority.

2.6. **The right to access and rectify data (Articles 109 and 110)**

Anyone is entitled to have access to data on him/herself and to ask that any errors be corrected. Such access shall be in accordance with the national law of the country in which the request is made.

A Member State may not authorise access to an alert issued by another Member State without first consulting the issuing Member State.

2.6.1. *The exchange of information regarding the right to access or rectify data*

If the national authorities are to be informed of a request to access or verify data, then the exchange of information will take place according to the following rules:

▼M2

The following procedure has been adopted:

(a) each Sirene bureau must apply its national legislation on the right to access to this 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 Member States concerned shall forward information on exercising this right to access.

2.6.2. *Information on requests for access for alerts issued by other Member States*

As far as is possible, information on alerts entered into the SIS by another Member State shall be exchanged via the national Sirene bureaux.

The following procedure has been adopted:

(a) the request for access shall be forwarded to the Member State that issued the alert as soon as possible, so that it can take a position on the question;

(b) the issuing Member State shall inform the Member State that received the request of its position;

(c) it shall take account of any legal deadlines set for processing the request.

If the Member State that issued the alert sends its position to the Sirene bureau of the Member State 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.

2.6.3. *Information on access and rectification procedures*

The following procedure has been adopted:

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. In this respect K-forms should be used.

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

Inform the Member States who had been unable to enter their alert that a hit has been made and that the alert has been deleted.

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 deletion message should be processed automatically by the N.SIS.

2.8. **Misused identity**

A misused identity (name, first-name, date of birth) occurs if an offender uses the identity of a real person. This can happen when a document is used to the detriment of the real owner.

The Member State issuing the code 3 in the field of ‘category of identity’ shall send the **Q form** at the same time as entering/modifying the alert into the SIS.

▼M2

If the code 3 is found in the field of 'category of identity' when the SIS is consulted, the official conducting the check should contact the national Sirene bureau and obtain additional information in order to clarify whether the person being checked is the person sought or the person whose identity is misused.

As soon as it is clear that a person's identity is misused a code 3 shall be set in the alert. The person involved should, according to national procedures, provide the national Sirene bureau of the issuing Member State with the information needed, such as genuine particulars, identity papers details and/or filling out the **Q form**.

Subject to the condition mentioned below, the photographs and fingerprints of the person whose identity is misused should also be on file at the Sirene bureau of the issuing Member State.

On the **Q form**, only the Schengen number refers to the data for the person sought by the SIS alert. The information in heading 052 (Date document was issued) is compulsory. Heading 083 (Particular information concerning the alert) should always indicate the contact service, which has further information on the alert.

This information can only be processed with the free and explicit permission of the person whose identity is misused.

Furthermore, on becoming aware that a person alerted in the SIS is misusing someone else's identity, the issuing State shall check whether it is necessary to maintain the misused identity in the SIS alert (to find the person sought).

The data of the person whose identity is misused shall only be available for the purpose of establishing the identity of the person being checked and shall in no way be used for any other purpose. Information on misused identity should be deleted after the deletion of the alert.

2.9. **Sirpit (Sirene Picture Transfer)**

2.9.1. *Development and background of Sirpit (Sirene Picture Transfer)*

Sirene bureaux should be able to exchange fingerprints and pictures for identification purposes.

The Sirpit procedure makes it possible, when there is some doubt about the identity of a discovered person, to exchange pictures and fingerprints quickly and electronically between Sirene bureaux, so that a comparison can be made between the fingerprints and pictures of the discovered person and those of the person regarding whom an alert was issued.

Within the framework of police cooperation, the exchange of pictures and fingerprints may also be carried out in the cases provided for by Articles 39 and 46 of the Convention Implementing the Schengen Agreement, on condition that the Sirene bureaux also handle these cases.

2.9.2. *Further use of the data exchanged, including archiving*

Any further use of pictures and fingerprints exchanged via Sirpit, including archiving, must comply with the provisions of Title VI of the Schengen Convention and more specifically Articles 126 and 129 thereof (and, where applicable, the provisions of Directive 95/46/EC) and with the legislation in force in that area in the States concerned.

2.9.3. *Technical requirements*

Every Sirene bureau should fulfil the Sirpit technical requirements.

▼M2

The Sirene bureau must be able to, on the one hand, electronically exchange requests for comparison or verification and the results and, on the other hand, electronically send their requests — without changes — to and receive results from their national identification service.

Fingerprints and pictures are sent in an attachment on an input screen, specially designed for Sirpit.

2.9.4. *The national identification service*

The national identification service only receives requests emanating from, and sends results to, its own national Sirene bureau.

2.9.5. *Use of the Sirene **L form***

The transmission (request for and result of a comparison) via Sirpit is announced by sending an **L form** through the usual channel used for all Sirene forms. **L forms** are sent at the same time as fingerprints and/or pictures.

In cases under Articles 39 and 46 of the Schengen Convention, the **L form** is replaced by an agreed form of announcement.

2.9.6. *Sirpit procedure*

The Sirene bureau of the country in which the person was discovered is known hereafter as 'the discovering Sirene bureau'.

The Sirene bureau of the country, which has introduced the alert into the SIS, is known hereafter as 'the providing Sirene bureau'.

The procedure allows for two possibilities:

2.9.6.1. The discovering Sirene bureau makes the comparison

(a) The discovering Sirene bureau sends a **G form** through the usual electronic path and asks, in field 089, the providing Sirene bureau to send an **L form** as soon as possible, as well as the fingerprints and pictures if these are available.

(b) The providing Sirene bureau replies in an **L form**. If the fingerprints and pictures are available, the providing Sirene bureau mentions in field 083 that fingerprints and/or pictures are sent in order to make the comparison.

(c) The discovering Sirene bureau sends the fingerprints and pictures to its national identification service for comparison, and asks for the result through the same path.

(d) The discovering Sirene bureau provides the result in an **L form** (in field 083) to the providing Sirene bureau.

2.9.6.2. The providing Sirene bureau makes the comparison

(a) The discovering Sirene bureau sends a **G form** and an **L form** through the usual electronic path and mentions in field 083 of the **L form** that the fingerprints and pictures are being sent for comparison.

(b) The providing Sirene bureau sends the fingerprints and pictures it has received to its national identification service for comparison and asks for the result through the same path.

(c) The providing Sirene bureau provides the result in an **L form** (in field 083) to the discovering Sirene bureau.

▼M2

After comparison, the fingerprints and pictures of a reported person may be kept in the file by the discovering Sirene bureau in case further comparisons are required

The fingerprints and pictures of a person not matching the data of the reported person which have been exchanged via Sirene must be processed in accordance with the provisions of Title VI of the Schengen Convention and more specifically Articles 126 and 129 thereof (and, where applicable, the provisions of Directive 95/46/EC) and with the legislation in force in that area in the States concerned. This should normally lead to the deletion of the fingerprints and pictures in question.

2.9.6.3. Input screen

The input mask will be developed with reference to the existing Interpol input mask (ANSI/NIST standard).

The mask will have the following data:

1. Schengen ID number (Articles 95 to 100) (*) ([11])
2. Reference number (Articles 39 or 46) (*) ([11])
3. Date of fingerprints
4. Date of picture
5. Reason for fingerprints (*) ([12])
6. Family name (*) ([13])
7. First name (*) ([13])
8. Maiden name
9. Identity ascertained?
10. Date of birth (*)
11. Place of Birth
12. Nationality
13. Gender (*)
14. Additional information
15. Remarks.

2.10. **Police cooperation (Articles 39 to 46)**

Police cooperation between the Member States shall not be limited to using the information in the SIS.

The following is recommended:

(a) that the Sirene bureaux of the Member States exchange any useful information whilst respecting any national measures taken to implement Articles 39 — 46 using SIS-NET e-mail; and

(b) that the Sirene bureaux keep each other informed of measures taken at national level, and of subsequent amendments to these measures.

A hit may lead to the discovery of an offence or a serious threat to public security. Accurate identification of a subject may be essential, and the exchange of information, e.g. photographs or fingerprints, is a particularly important factor. Articles 39 and 46 provide the authority for these exchanges which shall take

(*) Compulsory
([11]) An entry must be made in either Field 1 or Field 2.
([12]) An entry must be made only in accordance with Article 39 or 46 (Field 2).
([13]) The option ‘unknown’ may be entered.

▼M2

place in accordance with the provisions of Title VI of the Convention.

2.10.1. *Specific powers in policing and security matters. Title III. (Articles 39 and 46)*

Title III of the Schengen Convention contains a number of additional police and judicial cooperation provisions.

The following is recommended:

(a) that each Member State gives its Sirene bureau specific policing and security powers, in line with Title III of the Convention; and

(b) that the Member States shall inform each other of the measures taken at national level for respective Sirene bureaux, and of any subsequent amendments to these measure.

2.11. **Overlapping roles of Sirene and Interpol**

The role of the SIS is neither to replace nor to replicate the role of Interpol. Although tasks may overlap, the governing principles for action and cooperation between the Member States under Schengen differ substantially from those under Interpol. It is therefore necessary to establish rules for cooperation between the Sirene bureaux and the NCBs (National Central Bureaux) at national level.

The following principles have been agreed:

2.11.1. *Priority of SIS alerts over Interpol alerts*

SIS alerts and the exchange of all information on these alerts shall always have priority over alerts and information exchanged via Interpol. This is of particular importance if the alerts conflict.

2.11.2. *Choice of communication channel*

The principle of Schengen alerts taking precedence over Interpol alerts shall be respected and it shall be ensured that the NCBs of Member States comply with this as well. Once the Schengen alert is created, all communication related to the alert and the purpose for its creation, shall be provided by Sirene bureaux. If a Member State wants to change channels of communication, the other parties have to be consulted in advance. Such a change of channel is possible only in special cases.

2.11.3. *Use and distribution of Interpol in Schengen States*

Given the priority of SIS over Interpol alerts, Interpol alerts shall be restricted to exceptional cases (i.e. where there is no provision, either in the Convention or in technical terms, to enter the alert in the SIS, or where not all the necessary information is available to form 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’.

2.11.4. *Sending information to third States*

The Sirene bureau of the issuing Member State shall decide whether to pass information on to third States (authorisation, diffusion means and channel). In so doing the Sirene bureau shall observe the personal data protection provisions laid down in the Schengen Convention and Directive 95/46/EC. Use of the

▼M2

Interpol channel will depend on national provisions or procedures.

2.11.5. *Hit and deletion of an alert*

The Schengen States shall ensure at national level that the Sirene bureaux and the NCBs inform each other of hits.

The deletion of an alert shall be undertaken only by the authority, which issued the alert.

2.11.6. *Improvement of cooperation between the Sirene bureaux and the Interpol NCBs*

Each Member State shall take all appropriate measures to provide for effective exchange of information at national level between its Sirene bureau and the NCBs.

2.12. **Cooperation with Europol and Eurojust**

In order to streamline cooperation between Sirene bureaux, appropriate national procedures have to be established.

2.13. **Special types of search**

2.13.1. *Geographically targeted search*

A geographically targeted search is a search carried out in situation, that requesting country has firm evidence of the whereabouts of the wanted person or object within a restricted geographical area. In such circumstances a request from the judicial authority may be executed immediately on receipt.

Geographically targeted searches in the Schengen area shall take place on the basis of the alert in the SIS. The relevant M form, which is to be sent at the same time as the alert is created or the information on whereabouts is acquired, shall include information of whereabouts of the wanted person or object. An alert for the wanted person shall be entered in the SIS to ensure that a request for provisional arrest is immediately enforceable (Article 64 in the Convention, Article 9(3) of the Framework Decision on EAW).

Such an alert increases the chances of success should the person or object move unexpectedly from one place to another within the Schengen area, so the non entering of wanted person or object into SIS is possible only in special circumstances (e.g. there is not enough information to create an alert etc.).

2.13.2. *Search with participation of special police units of targeted search*

The services provided by special units that conduct targeted searches should also be used in suitable cases by Sirene bureaux in requested Member States. Therefore good cooperation with such units has to be established and the exchange of information ensured. The alert in SIS cannot be replaced by international cooperation of the abovementioned police units. Such cooperation shall not collide with the Sirene bureau's role as a focal point for searches using SIS.

2.14. **Adding a flag**

At the request of another Member State to add a flag

Articles 94(4), 95(3), 97 and 99(6) allows a requested Member State to refuse to carry out the prescribed procedure on its territory by requesting a flag be added to the mentioned Article 95, 97 or 99 alert. The reasons for the request shall be provided simultaneously.

▼M2

2.14.1. *The exchange of information when adding a flag*

The Sirene bureaux shall exchange information so that Member States can assess the need for a flag.

A flag may be added (or deleted) at any time under the terms of Article 94(4) on alerts pursuant to Article 95, Article 97 and Article 99 alerts. When a flag is added to Articles 97 and 99 alerts the alert does not appear on the screen when the end user consults the system. An alternative procedure exists for Article 95 alerts. Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

2.14.2. *Consulting the Member States with a view to adding a flag*

The following procedure has been adopted:

(a) if a Member State requires a flag to be added, it should request the flag from the issuing Member State, mentioning the reason for the flag;

(b) once information has been exchanged, the alert may need to be amended, deleted or the request may be withdrawn

2.14.3. *A request for a flag to be added*

The following procedure has been adopted:

(a) the requested Member State asks the Member State that issued an Article 95, 97 or 99 alert to add a flag. This request shall be made by using **F form**;

(b) the Member State that issued the alert is obliged to add the requested flag immediately.

2.14.4. *Systematic request for a flag to be added for a Member State's nationals*

The following procedure has been adopted:

(a) a Member State may ask the Sirene bureau of the other Member State to add a flag as a matter of course to Article 95 alerts issued on its nationals;

(b) any Member State wishing to do so shall send a written request to the Member State, which it would like to cooperate;

(c) any Member State to whom such a request is addressed shall add a flag for the Member State in question immediately after the alert is issued;

(d) this procedure shall continue to be binding until a written instruction is made for it to be cancelled.

If the circumstances mentioned in Article 94(4) no longer exist, the Member State that requested the flag must ask as soon as possible for the flag to be revoked.

3. **ALERTS PURSUANT TO ARTICLE 95** ([14])

The following steps have to be followed:

— Member State checks prior to issuing the alert,

— multiple alerts,

— supplementary information to be sent to Member States,

— at the request of another Member State add a flag,

— action by Sirene bureau upon receipt of an Article 95 alert,

— the exchange of information after a hit,

([14]) 'Persons wanted for arrest for extradition'.

▼M2

— deletion of an alert,

— misused identity.

3.1. **Member State checks prior to issuing the alert**

Most newly issued Article 95 alerts will be accompanied by a European Arrest Warrant (EAW). However, under an Article 95 alert it is also possible for provisional arrest prior to obtaining an international arrest warrant (IAW). The checks required before each of these cases are as follows:

The EAW/IAW must be issued by a judicial authority authorised to carry out this function in the issuing Member State.

There should be sufficient detail contained in the EAW/IAW and in the **A form** (in particular, EAW section (e): 'description of the circumstances in which the offence(s) was (were) committed, including the time and place' and **A form**, field 044: 'description of the deeds') for other Sirene bureaux to verify the alert.

3.2. **Checking whether the national law of the Member States authorises arrest with a view to surrender or extradition**

The Member State issuing an alert shall check whether the arrest that is to be requested is authorised by the national law of the other Member States.

The following procedure has been adopted:

(a) check that all Member States are able to follow up the alert.

(b) if there is any doubt, consult the Sirene bureau concerned and transmit or exchange the information necessary for the check.

Each Member State shall take appropriate technical or organisational measures to ensure that alerts pursuant to the second sentence of Article 95(2) are only entered into the SIS after the Sirene bureau of the Member State in question has been informed.

3.3. **Multiple alerts**

3.3.1. *Check for multiple alerts (Article 107)*

Each Member State can only enter one alert on the system per wanted person. Therefore, a check is required to identify multiple requests for an alert from one Member State. In the event of multiple requests by one Member State, a national procedure is required to agree which EAW will be shown on the Article 95 alert. Alternatively, a single EAW could be issued to cover all offences.

Several alerts issued by different countries for the same subjects may sometimes occur. Therefore, this calls for:

(a) checks before entering an alert, to determine whether the subject is already in the SIS;

(b) consultation with other Member States, when the entry of an Article 95 alert will cause multiple alerts that are incompatible (for example, if an Article 99 Alert already exists for that person and an Article 95 should be entered).

Article 95 alerts are compatible with Article 97 and 98 alerts. They may also co-exist with Article 96 alerts, although in such cases, the Article 95 procedures have priority over those set for Article 96. Article 99 alerts are not compatible with Article 95 alerts.

The order of priority for alerts is as follows:

▼M2

— arrest with a view to surrender or 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).

Departures from this order of priority may be made after consultation between the Member States if essential national interests are at stake.

The Sirene bureau of the Member State issuing an alert shall maintain a record of any requests to enter a further alert which, after consultation, have been rejected by virtue of the provisions given above, until the alert is deleted.

Whenever a hit occurs in a Member State, the Sirene bureau of the Member State that produced the alert may send as many EAW as have been issued by their competent judicial authorities.

Several Member States may enter an alert for an EAW on the same person. If two or more Member States have issued an EAW for the same person, the decision on which warrant shall be executed in the event of an arrest shall be taken by the executing judicial authority in the Member State where the arrest occurs.

3.3.2. *Exchange of information*

To avoid entering incompatible multiple alerts, care must be taken to distinguish accurately between individuals who have similar characteristics.

Consultation and cooperation between the Sirene bureaux are therefore essential, and each Member State shall establish appropriate technical procedures to detect such cases before an entry is made.

The elements used for establishing whether two identities may 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 a person 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 national requesting department to clarify whether the alert relates to the same person

(c) if the check reveals that the details are identical and could relate to the same person, the Sirene bureau shall apply the procedure for entering multiple alerts. If the outcome of the check is that the details relate to two different people, the Sirene bureau shall approve the request for entering the new alert.

3.3.3. *Entering an alias*

(a) In order to avoid incompatible alerts of any category due to an alias to be entered, the concerned Member States should inform each other about this alias and transmit all relevant information about the real identity of the searched subject.

▼M2

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 Member States of aliases regarding an alert issued pursuant to Article 95.

(c) Enter the alert into the SIS.

3.4. **Supplementary information to be sent to Member States**

3.4.1. *Supplementary information to be sent with regards to an EAW*

The **A** and **M forms**, which are uniform for all Member States, should be used and the information contained in these forms should be the same as that in the EAW.

In an **A form**:

— 006-013: the relevant information inserted in the SIS and corresponding to section (a) of the EAW should be entered,

— 030: information that this **A form** is specific to an EAW should be entered along with details of the magistrate or court ordering the arrest warrant, taken from section (i) of the EAW,

— 031: the relevant information contained in the EAW section (b) concerning the decision on which the warrant is based should be entered,

— 032: the date of the arrest warrant should be entered,

— 033: the capacity of the judicial authority which issued the warrant should be entered, taken from section (i) of the EAW,

— 034: the relevant information from the EAW section (c, 1) plus, where applicable:

  — the offence(s) on the basis of which the warrant has been issued is (are) punishable by a custodial life sentence or lifetime detention order,

  — the legal system of the issuing Member State allows for a review of the penalty or measure imposed, on request or at least after 20 years, aiming at a non-execution of such penalty or measure,

  and/or

  — the legal system of the issuing Member State allows for the application of measures of clemency to which the person is entitled under the law or practice of the issuing Member State, aiming at a non-execution of such penalty or measure,

— 035-037: the relevant information from the EAW section (b) should be entered,

— 038: the relevant information from the EAW section (c, 2) plus, where applicable

  — the offence(s) on the basis of which the warrant has been issued is (are) punishable by a custodial life sentence or lifetime detention order,

  — the legal system of the issuing Member State allows for a review of the penalty or measure imposed, on request or at least after 20 years, aiming at a non-execution of such penalty or measure,

▼M2

and/or

— the legal system of the issuing Member State allows for the application of measures of clemency to which the person is entitled under the law or practice of the issuing Member State, aiming at a non-execution of such penalty or measure,

— 039: information from EAW section (c, 2) should be entered,

— 040: information from EAW section (e) on the applicable statutory provision/code,

— 041: information from EAW section (e) on the nature and legal classification of the offence(s),

— 042: information from EAW section (e) on the time the offence(s) was (were) committed,

— 043: information from EAW section (e) on the place the offence(s) was (were) committed,

— 044: information from EAW section (e) on the circumstances of the offence(s),

— 045: information from EAW section (e) on the degree of participation by the requested person,

— 058: information from the EAW section (a) on distinctive marks/description of the person.

In an **M form**:

— 083: Where the text '*Information on decision rendered in absentia according to EAW section (d)*' appears, it is requested, where applicable:

(a) to reply if the decision was pronounced in absentia;

(b) if so, to specify whether the person concerned was personally summoned or informed of the date and place of the hearing where the decision was pronounced in absentia. If this is not the case, mention the legal safeguards.

Where the text 'Punishable offence(s) according to EAW section (e, I and II)' appears, one or more of the offences punishable in the issuing Member State by a custodial sentence or detention order of a maximum of at least three years as defined by the laws of the issuing Member State according to Article 2(2) of the Framework decision (or section (e)] of the EAW) has to be filled in, if applicable.

If the offence(s) does (do) fall within the list given in Article 2(2) of the framework decision concerning the EAW, the offence(s) must be entered in full into the **M form**, according to the wording used in the list.

If the offences do not fall within the list mentioned above, the following information is required:

(a) either that the warrant has been issued for acts punishable by the law of the issuing Member State by a custodial sentence or a detention order for a maximum period of at least twelve months;

(b) or, where a sentence has been passed or a detention order has been made, that the sentence is of at least four months.

In case the information to be inserted into field 083 of the **M forms** exceeds 1 024 characters, one or more supplementary **M forms** have to be sent.

▼M2

3.4.2. *Supplementary Information to be sent with regards to provisional arrest*

The file provided with regard to persons wanted for arrest for extradition purposes, shall be prepared before the alert is entered. A check should be made to ensure that the information is complete and correctly presented. The following information is to be provided: the details for prosecution or the enforcement of criminal sentences shall, in principle, be provided 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 Gender,

— 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’ and 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 No,

— 038 Sentence given,

— 039 Indication of sentence remaining to be served,

— 040 Legal texts applicable,

— 041 Legal description of the deed,

— 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.

The information given must be in sufficient detail for the other Sirene bureaux to verify the alert, but not in so much detail as to overload the message system.

▼M2

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 **A form** or heading 083 of **M form**).

3.4.3. *Further information to establish a person's identity*

The Sirene bureau of the issuing Member State may also, if necessary, provide further information, after consultation and/or at the request of another Member State, to help establish a person'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 alerts 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 and permanently accessible to them for speedy transmission.

The common objective is to minimise the risk of wrongly detaining a person whose details are of similar identity to those of the person on whom an alert has been issued.

3.4.4. *Sending the* A *and* M forms

The information mentioned in 3.3.1, 3.3.2 should be sent by the swiftest means available. The issuing Member State shall send the A and M forms at the same time as entering the Article 95(2) alert into the SIS. Any further information required for identification purposes shall be sent after consultation and/or at the request of another Member State. Multiple **A** and **M forms** describing different EAWs/IAWs can be sent if necessary.

3.5. **At the request of another Member State to add a flag**

Article 95(3) allows a requested Member State to refuse to carry out the prescribed procedure on its territory by requesting a flag to the Article 95 alert. The reasons for the request shall be provided simultaneously.

3.5.1. *The exchange of information when adding a flag*

The Sirene bureaux shall exchange information so that Member States can assess the need for a flag.

A flag may be added (or deleted) at any time under the terms of Article 94(4). Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

3.5.2. *Consulting the Member States with a view to adding a flag*

The following procedure has been adopted:

(a) if a Member State requires a flag to be added, it should request the flag from the issuing Member State, mentioning the reason for the flag;

▼M2

(b) once information has been exchanged, the alert may need to be amended, deleted or the request may be withdrawn.

3.5.3. *A request for a flag to be added*

The following procedure has been adopted:

(a) the requested Member State asks the Member State that issued an Article 95 alert to add a flag. This request shall be made by using an **F form**;

(b) the Member State that issued the alert is obliged to add the requested flag immediately.

3.5.4. *Systematic request for a flag to be added to a Member State's nationals*

The following procedure has been adopted:

(a) a Member State may ask the Sirene bureaux of the other Member States to add a flag as a matter of course to Article 95 alerts issued on its nationals where permitted;

(b) any Member State wishing to do so shall send a written request to the Member States, which it would like to cooperate;

(c) any Member State(s) to whom such a request is addressed shall add a flag for the Member State in question immediately after the alert is issued;

(d) this procedure shall continue to be binding until a written instruction is made for it to be cancelled.

If the circumstances mentioned in Article 95(2) no longer exist, the Member State that requested the flag must ask as soon as possible for the flag to be revoked.

3.6. **Action by Sirene bureaux upon receipt of an Article 95 alert**

When a Sirene bureau receives the **A** and **M forms**, the bureau or associated unit should, as soon as practicable, search all available sources to try and locate the subject. If the information provided by the requesting Member State is not sufficient for acceptance by the receiving Member State, this should not prevent the searches being carried out.

If the Article 95 alert is validated and the subject is located or arrested in the Member State, then the EAW and/or **A and M forms** should be forwarded to the authority of the Member State which executes the EAW. If the original EAW is requested, it should be sent by the issuing judicial authority direct to the executing judicial authority (unless otherwise directed).

3.7. **The exchange of information after a hit**

3.7.1. *Informing the Member States if an alert is matched*

The following procedure has been adopted:

(a) a hit on an individual on which an Article 95 alert has been issued should always be communicated to the Sirene bureau of the issuing Member State.

If necessary the Sirene bureau of the issuing Member State shall then send any relevant, specific information and the particular measures that should be taken to the Sirene bureau of the Member State that matched the alert.

When notifying the party, 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 a **G form**.

▼M2

If the hit concerns a person who is the subject of an Article 95 alert, the Sirene bureau of the Member State that matched the alert should inform the Sirene bureau of the issuing Member State of the hit by telephone after sending a **G form**;

(b) a Member State which had previously indicated a wish to issue an alert on a person or object already the subject of an alert should be informed of any hits on the original alert by the Member State that actually issued that alert;

(c) C.SIS automatically communicates the deletion of an alert to all Member States. It is therefore possible for a Member State to consider entering an alert, which was previously considered incompatible with an alert, which has now been deleted.

3.7.2. *Communicating further information*

The following procedure has been adopted:

(a) the Sirene bureaux may transmit further information on 95 to 100 alerts, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance;

(b) 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. Appropriate measures have to be taken by every Member State in order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46.

3.7.3. *Following a hit*

The end user may require the Sirene bureau to supply supplementary information to allow effective implementation of the procedures laid down in SIS tables 4, 10 or 16 as set out in Annex 4.

Unless stated otherwise, the issuing Member State must be informed of the hit and its outcome.

This procedure has technical implications, as the alert then has to be processed. It may need to be deleted, which may mean that another alert, which had previously been excluded from the system, can now be entered.

3.8. **Deletion of an alert**

Inform the Member States who had been unable to enter their alert that a hit has been made and that the alert has been deleted.

3.8.1. *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 has 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.

▼M2

The Sirene bureau is notified automatically by a message from its N.SIS that an alert put on hold can be entered.

The Sirene bureau shall apply the entire procedure for entering an alert in the appropriate alert category.

3.9. **Misused identity**

Reference should be made to point 2.8 on misused identity.

3.9.1. *Gathering and communicating information on the person whose identity is misused*

As soon as it's clear that a person's identity is misused a code 3 shall be set in the alert. The person involved should provide his/her national Sirene bureau with the information needed, such as genuine particulars, identity papers details and/or filling in the **Q form**.

Subject to the condition mentioned below, the photographs and fingerprints of the person whose identity is misused should also be on file at the Sirene bureau.

On the **Q form**, only the Schengen number refers to the data for the person sought by the SIS alert. The information in heading 052 (Date document was issued) is compulsory. Heading 083 (Particular information concerning the alert) should always indicate the contact service, which has further information on the alert.

This information can only be processed with the free and explicit permission of the person whose identity is misused.

Furthermore, on becoming aware that a person alerted in the SIS is usurping someone else's identity, the issuing State shall check whether it is necessary to maintain the misused identity in the SIS alert (to find the person sought).

3.9.2. *Communicating information on a person whose identity is misused*

The data of the person whose identity is misused shall only be available for the purpose of establishing the identity of the person being checked and shall in no way be used for any other purpose.

4. **ALERTS PURSUANT TO ARTICLE 96** ([15])

The following steps have to be followed:

— Introduction

— Check for multiple alerts, reference is made to General Procedures 2.1

— The exchange of information after a hit

— Misused identity, reference is made to the General Procedures 2.8

— Sirpit procedure, reference is made to General Procedures 2.9

4.1. **Introduction**

The exchange of information on third country nationals on whom an alert has been issued under Article 96 allows Member States to decide in the case of entry or visa application. If the subject is already on the territory of the Member State, it allows them to take the appropriate action for issuing residence-permits or expulsion:

([15]) Third country nationals for whom an alert has been issued for the purposes of refusing entry (Articles 2, 25, 96).

▼M2

The Member State, which reports the hit, may require background information on the alert and can ask the issuing Member State to provide the following information:

— Type of, and reason for, decision

— Authority issuing the decision

— Date of decision

— Date of service

— Date of enforcement

— Date of expiry of decision or length of validity

The notification procedures laid down under Article 5(2) and the consultation procedures laid down under Article 25 fall within the jurisdiction of the authorities responsible for issuing residence permits or visas. The Sirene bureaux shall not be involved in these procedures except to transmit supplementary information directly relating to the alerts (e.g. notification of a hit, clarification of identity) or to erase alerts.

However, the Sirene bureaux may be involved in transmitting supplementary information necessary for expulsion of, or for refusing entry to, a third country national, or in transmitting information generated by these actions.

The Sirene bureaux are also used as central authorities for transmitting and receiving additional information in the consultation procedure provided for in Article 25(1) and (2), and shall exchange **N forms** (Article 25(1)) and **O forms** (Article 25(2)) and at the request of the authorities responsible for issuing residence permits or visas with a view to retaining or deleting the alert.

If a Member State which grants a residence permit finds that the holder of the permit is the subject of an Article 96 alert, issued by another Member State, it shall inform their Sirene bureau (by fax, **M form**, etc), This Sirene bureaux shall then instigate the consultation procedure laid down in Article 25 (2) using the form provided for this purpose.

If a third Member State, i.e. neither that which granted the residence permit nor that which issued the alert, considers that there are grounds for consultation, it shall notify both the Member States which granted the permit and the Member State which issued the alert.

4.2. **Alerts pursuant to Article 96**

Enter the alert into the SIS.

4.3. **Entering an alias**

In order to avoid incompatible alerts of any category due to alias to be entered the concerned Member States should inform each other about this alias and transmit all relevant information about the real identity of the searched subject.

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.

4.4. **Misused identity**

If the code 3 is found in the field of ‘category of identity’ when the SIS is consulted, the official conducting the check should contact the national Sirene bureau and obtain additional infor-

▼M2

mation in order to clarify whether the person being checked is the person sought or the person whose identity is misused.

4.4.1. *Gathering and communicating information on a person whose identity is misused*

See point 2.8 on misused identity

4.5. **Issuing residence permits or visas**

The following procedure has been adopted:

(a) a requested Member State may inform the Member State which issued an alert pursuant to Article 96 of its having been matched. The Member State that issued the alert may then inform the other Member States if it thinks so fit;

(b) if so requested, and whilst respecting national legislation, the Sirene bureaux of the Member States 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. **Refusing admission or expulsion from Schengen territory**

The following procedure has been adopted:

(a) a Member State may ask to be informed of any alerts it issued pursuant to Article 96 that have been matched.

Any Member State that wishes to take up this option shall ask the other Member States in writing;

(b) a requested Member State may take the initiative and inform the Member State issuing an alert pursuant to Article 96 that the alert has been matched, that the third country national has not been granted admission or has been expelled from Schengen territory;

(c) if, on its territory, a Member State intercepts a person for whom an alert has been issued, the Member State issuing the alert may forward the information required to expel (return/deport) a third-country national. Depending on the needs of the discovering Member State and if available to the requested Member State, this information should include the following:

— the type and reason 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.

If a person on whom an alert has been issued is intercepted at the border the procedures set by the issuing Member State 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 Member States concerned via the Sirene bureaux.

▼M2

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 on third country nationals not to be granted admission**

If a third country national 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 Member States 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.

4.8. **Informing the Schengen Member States if an alert is matched**

The Sirene bureaux of Member States that have issued alerts under Article 96 shall not necessarily be informed of any hits as a matter of course, but may be informed in exceptional circumstances.

However, Sirene bureaux should provide statistics on hits.

Every hit should be accurately registered, including those on alerts pursuant to Article 96. A distinction should be made between hits found on alerts issued by another Member State and hits found by a Member State on alerts issued by itself. Hits should be categorised per article.

5. **ALERTS PURSUANT TO ARTICLE 97** ([16])

The following steps have to be followed/considered:

— Check for multiple alerts, reference is made to General Procedures 2.1

— At the request of another Member State add a flag

— The exchange of information after a hit

— Misused identity, reference is made to General Procedures 2.8

— Sirpit procedure, reference is made to the General Procedures 2.9

5.1. **Alerts pursuant to Article 97**

(a) Enter the alert into the SIS.

(b) At the request of a Member State add a flag.

5.2. **Adding a flag**

Articles 94(4), allow a requested Member State to refuse to carry out the prescribed procedure on its territory by requesting a flag be added to the alert in question. This may apply to alerts issued by virtue of Articles 97. The reasons for the request shall be provided simultaneously.

5.2.1. *The exchange of information when adding a flag*

The Sirene bureaux shall exchange information so that Member States can assess the need for a flag.

([16]) Missing persons or persons who, for their own protection or in order to prevent threats, need temporarily to be placed under police protection.

▼M2

A flag may be added (or deleted) at any time under the terms of Article 94(4) on alerts pursuant to Article 95, Article 97 and Article 99 alerts. When a flag is added on Article 97 and 99 alerts the alert does not appear on the screen when the end user consults the system. An alternative procedure exists for Article 95 alerts. Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

5.2.2. *Consulting the Member States with a view to adding a flag*

The following procedure has been adopted:

(a) if a Member State requires a flag to be added, it should request the flag from the issuing Member State, mentioning the reason for the flag.

(b) once information has been exchanged, the alert may need to be amended, deleted or the request may be withdrawn.

5.2.3. *A request for a flag to be added*

The following procedure has been adopted:

(a) the requested Member State asks the Member State that issued an Article 95, 97 or 99 alert to add a flag. This request shall be made by using an **F form**;

(b) the Member State that issued the alert is obliged to add the requested flag immediately.

5.3. **After a hit**

The end-user may require the Sirene bureau to supply supplementary information to allow effective implementation of the procedures laid down in SIS tables 4, 10 or 16 as set out in Annex 4.

Unless stated otherwise, the issuing Member State must be informed of the hit and its outcome.

This procedure has technical implications, as the alert then has to be processed. It may need to be deleted, which may mean that another alert, which had previously been excluded from the system, can now be entered.

5.3.1. *Communicating further information*

The following procedure has been adopted:

(a) the Sirene bureaux may transmit further information on 95 to 100 alerts, and in doing so may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance;

(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. Appropriate measures have to be taken by every Member State in

▼M2

order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46.

6. **ALERTS PURSUANT TO ARTICLE 98** ([17])

6.1. **Alerts pursuant to Article 98**

The following steps have to be followed/considered:

— Check for multiple alerts, reference is made to General Procedures 2.1

— The exchange of information after a hit

— Misused identity, reference is made to general procedures 2.8

— Sirpit procedure, reference is made to the General Procedures 2.9

— Enter the alert into the SIS

6.2. **After a hit**

The end-user may require the Sirene bureau to supply supplementary information to allow effective implementation of the procedures laid down in SIS tables 4, 10 or 16 as set out in Annex 4.

Unless stated otherwise, the issuing Member State must be informed of the hit and its outcome.

This procedure has technical implications, as the alert then has to be processed. It may need to be deleted, which may mean that another alert, which had previously been excluded from the system, can now be entered.

6.2.1. *Communicating further information*

The following procedure has been adopted:

(a) the Sirene bureaux may transmit further information on 95 to 100 alerts, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance;

(b) 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. Appropriate measures have to be taken by every Member State in order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46.

7. **ALERTS PURSUANT TO ARTICLE 99** ([18])

The following steps have to be followed/considered:

— Pre-check in order to guarantee the consultation process

— Check for multiple alerts, reference is made to General Procedures 2.1

— At the request of another Member State add a Flag

— The exchange of information after a hit

([17]) Data on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings.

([18]) Persons or vehicles for the purpose of discreet surveillance or of other specific checks.

▼M2

— Sirpit procedure, reference is made to General Procedures 2.9

7.1. **Alerts pursuant to Article 99(2)**

(a) Enter the alert into the SIS.

(b) At the request of another Member State add a flag.

7.2. **Entering an alias**

(a) In order to avoid incompatible alerts of any category due to alias to be entered the concerned Member States should inform each other about this alias and transmit all relevant information about the real identity of the searched subject. 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 Member States of aliases regarding an alert issued pursuant to Article 99. 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.

7.3. **Consulting the Member States prior to alerts on grounds of State security**

A Member State planning to issue an alert for the purposes of discreet surveillance or of a specific check on the grounds of State security shall consult the other Member States before doing so.

A specific procedure is required to safeguard the confidentiality of certain information, and any contact between the services responsible for State security should therefore be kept quite separate from the contact between the Sirene bureaux.

In each case, the Sirene bureau shall ensure that the consultation procedure functions smoothly and shall record the results. The information itself shall be 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. The purpose of this is mainly to establish whether there are any objections to the planned alert.

(b) Following the exchange of information, the security department wishing to enter the alert forwards the results of the information exchange to its national Sirene bureau.

(c) The Sirene bureau shall inform the other Sirene bureau, so allowing the other Sirene bureaux to consult their respective security departments (**M form**).

(d) Once the Sirene bureau of the issuing Member State has established that the consultation process has been properly completed, it shall approve the entry of the alert.

(e) Should a Member State perceive a difficulty with the establishment of the alert, its Sirene bureau shall inform the issuing Member State.

(f) If the issuing Member State wishes to maintain the alert, the requested Member State may ask that a flag be entered. This shall be withdrawn if, after full consideration, it is found to be unnecessary. Otherwise it shall be retained,

▼M2

thereby suspending the course of action that should normally be followed for the alert.

7.4. **Adding a flag**

Article 99 allows a requested Member State to refuse to carry out the prescribed procedure on its territory by requesting a flag to the alert in question. This may apply to alerts issued by virtue of Articles 99. The reasons for the request shall be provided simultaneously.

7.4.1. *The exchange of information when adding a flag*

The Sirene bureaux shall exchange information so that Member States can assess the need for a flag.

A flag may be added (or deleted) at any time under the terms of Article 94(4) on alerts pursuant to Articles 95, 97 and 99 alerts. When a flag is added to Articles 97 and 99 alerts the alert does not appear on the screen when the end user consults the system. An alternative procedure exists for Article 95 alerts. Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

7.4.2. *Consulting the Member States with a view to adding a flag*

The following procedure has been adopted:

(a) if a Member State requires a flag to be added, it should request the flag from the issuing Member State, mentioning the reason for the flag;

(b) once information has been exchanged, the alert may need to be amended, deleted or the request may be withdrawn.

7.4.3. *A request for a flag to be added*

The following procedure has been adopted:

(a) the requested Member State asks the Member State that issued an Article 95, 97 or 99 alert to add a flag. This request shall be made by using an **F form;**

(b) the Member State that issued the alert is obliged to add the requested flag immediately.

7.5. **Communicating further information following a hit**

The following procedure has been adopted:

(a) the Sirene bureaux may transmit further information on 95 to 100 alerts, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance;

(b) of 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. Appropriate measures have to be taken by every Member State in order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46;

(c) When a positive hit occurs on an Article 99(3) alert, the discovering Sirene bureau will inform the counterpart (requesting Sirene bureau) of the results (discreet surveillance or specific check) via the **G form**. At the same time the discovering Sirene bureau will inform its own competent service responsible for State security.

▼M2

If the State security service in the discovering Member State decides that the alert requires a validity flag, they should contact their national Sirene bureau in order to raise the flag with the requesting Sirene bureau (via the **F form**). They are not required to explain the reasons for raising the flag, but the request should be made through Sirene channels.

A specific procedure is required to safeguard the confidentiality of certain information. Therefore, any contact between the services responsible for State security should be kept quite separate from the contact between the Sirene bureaux. Consequently, the reasons for requesting a flag should be discussed directly between State security services and not through Sirene bureaux.

8. **ALERTS PURSUANT TO ARTICLE 100** ([19])

The following steps have to be followed/considered:

— Check for multiple alerts

— The exchange of information after a hit

— Sirpit procedure, reference is made to General Procedures 2.9

8.1. **Vehicle alerts pursuant to Article 100**

8.1.1. *Checking for multiple alerts on a vehicle*

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

— the registration/number plate, and/or

— the serial number.

Both numbers may feature in the SIS.

Checks for multiple alerts are made by comparing numbers. If, when entering a new alert, it is found that the same serial number and/or registration plate number already exist in the SIS, it is assumed that the new alert will result in multiple alerts on the same vehicle. However, this method of verification is effective only where the description elements used are the same and comparison is therefore not always possible.

The Sirene bureau shall draw the national users' attention to the problems which may arise where only one of the numbers has been compared a positive response does not mean automatically that there is a hit, and a negative response does not mean that there is no alert on the vehicle.

The identity description elements used for establishing whether two vehicle entries are identical are detailed in Annex 6 of this manual.

The consultation procedures to be adopted by the Sirene bureaux for vehicles are the same as for persons.

8.1.2. *The specific case of alerts on vehicles*

The following general recommendations have been adopted:

(a) Only one alert per Member State may be entered in the SIS for any one vehicle;

(b) Several Member States may enter an alert on the same vehicle if the alerts are compatible or may coexist;

([19]) Objects sought for the purpose of seizure or use as evidence in criminal proceedings.

▼M2

(c) Within Article 99, alerts on vehicles issued for 'discreet surveillance' are incompatible with those issued for 'specific checks' (**E form)**.

(d) Article 99 alerts are incompatible with Article 100 alerts.

(e) The Sirene bureau of the Member State issuing an alert shall maintain an alert of any requests to enter a further alert which, after consultation, have been rejected by virtue of the provisions given above, until the alert is deleted.

Table of compatible alerts

Priority by decreasing order of importance	Grounds for alert compatibility
Article 99 Discreet surveillance	Article 99 discrete surveillance
Article 99 Specific check	Article 99 specific check
Article 100	Article 100

8.2. **Communicating further information following a hit**

The following procedure has been adopted:

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

(b) 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. Appropriate measures have to be taken by every Member State in order to guarantee an efficient and effective exchange of complementary information by virtue of Articles 39 and 46.

The Sirene bureaux shall send further information as quickly as possible via 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, e.g.: 041, 042, 043, 162, 164, 165, 166 and 167).

9. **STATISTICS**

Once a year the Sirene bureaux will provide hit statistics. The statistics will cover all the articles and the types of alerts. The statistics report is to be sent electronically to the General Secretariat of the Council.