ANNEX

SIRENE MANUAL

INTRODUCTION

On 14 June 1985, the Governments of 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'.

The five founding countries signed the Convention implementing the Schengen Agreement[(1)] on 19 June 1990, and were later joined by the Italian Republic on 27 November 1990, the Kingdom of Spain and the Portuguese Republic on 25 June 1991, the Hellenic Republic on 6 November 1992, the Republic of Austria on 28 April 1995 and by the Kingdom of Denmark, the Kingdom of Sweden and the Republic of Finland on 19 December 1996.

The Kingdom of Norway and the Republic of Iceland also concluded a Cooperation Agreement with the Member States on 19 December 1996, in order to join this Convention.

Subsequently, as of 26 March 1995, the Schengen *acquis* was fully applied in Belgium, Germany, France, Luxembourg, Netherlands, Spain and Portugal[(2)]. As of 31 of March 1998, in Austria and Italy[(3)]; as of 26 of March 2000 in Greece[(4)] and finally, as of 25 March 2001, the Schengen *acquis* was applicable in full in Norway, Iceland, Sweden, Denmark and Finland[(5)].

The United Kingdom (UK) and Ireland only take part in some of the provisions of the Schengen Acquis, in accordance with Council Decision 2000/365/EC[(6)] and Council Decision 2002/192/EC[(7)] respectively.

In the case of the UK, the provisions of the Schengen *acquis* in which the United Kingdom takes part are applicable as of the 1 January 2005[(8)], with the exception of the provisions on the Schengen Information System.

The Schengen *acquis* was incorporated into the legal framework of the European Union by means of protocols attached to the Treaty of Amsterdam[(9)] in 1999. A Council Decision was adopted on 12 May 1999, determining the legal basis for each of the provisions or decisions which constitute the Schengen *acquis*, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union.

From 1 May 2004, the Schengen *acquis*, as integrated into the framework of the European Union by the Protocol annexed to the Treaty on European Union and to the Treaty establishing the European Community (hereinafter referred to as the 'Schengen Protocol'), as well as the acts building upon it or otherwise related to it are binding on the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic. As of 1 January 2007, this also applies to the Republic of Bulgaria and to Romania.

In December 2007, the Council adopted a Decision on the full application of the provisions of the Schengen *acquis* in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic[(10)]. Accordingly, controls at internal land and sea borders of these Member States were lifted in December 2007 and at internal air borders in March 2008.

As regards the Republic of Bulgaria and Romania, Council Decision 2010/365/EU[(11)] allows for real SIS data to be transferred to the Member States concerned. The concrete use of this data allows the Council, through the applicable Schengen evaluation procedures, as set out in SCH/Com-ex (98) 26 def., to verify the correct application of the provisions of the Schengen *acquis* relating to the SIS in the Member States concerned. Once these evaluations have been carried out, the Council should decide on the lifting of checks at the internal borders with those Member States.

As regards Switzerland, an Agreement was concluded by the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen *acquis*[(12)]. Controls at internal land borders of Switzerland were lifted in December 2008 and at internal air borders in March 2009, in accordance with the relevant decision of the Council[(13)].

As regards Liechtenstein, a Protocol was signed between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[(14)].

1. THE SCHENGEN INFORMATION SYSTEM (SIS) AND THE NATIONAL SIRENE BUREAUX

The SIS, together with the cooperation of the SIRENE bureaux, set up pursuant to the provisions of Title IV of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (Schengen Convention)[(15)] constitutes an essential tool for the application of the provisions of the Schengen *acquis* as integrated into the framework of the European Union.

The Schengen Information System (SIS) shall provide access to alerts on persons and objects to the following authorities:

(a) authorities responsible for border checks;

(b) authorities carrying out and coordinating other police and customs checks within the country;

(c) national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation;

(d) authorities responsible for issuing visas, the central authorities responsible for examining visa applications, authorities responsible for issuing residence permits and for the administration of legislation on third-country nationals in the context of the application of the Union *acquis* relating to the movement of persons;

(e) authorities responsible for issuing vehicle registration certificates.

Europol and Eurojust also have access to certain categories of alerts[(16)]. Europol may access data entered in accordance with Article 95 (alerts for arrest), Article 99 (alerts for discreet surveillance or specific check) and Article 100 (alerts on objects for seizure or use as evidence in criminal proceedings). Eurojust may access data entered in accordance with Article 95 (alerts for arrest) and Article 98 (alerts for a judicial procedure).

The SIS is made up of separate components: the technical support function (C.SIS) and the national sections (N.SIS, one for each Member State), connected by a network (SISNET). 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 Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

1.1. The SIRENE bureaux[17]

Article 92(4) of the Schengen Convention provides that Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (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 this System.

To meet the operating constraints set out in the Schengen Convention, every Member State shall 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 the SIRENE bureau, shall be fully operational on a 24/7 basis.

1.2. 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.

1.3. Standards

The following fundamental standards that underpin the cooperation via SIRENE shall be met:

1.3.1. *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 SIS-related provisions of the Schengen Convention. It shall be fully operational with sufficient capacity 24 hours a day, 7 days a week. Availability for technical analysis, support and solutions shall also be provided with sufficient capacity 24 hours a day, 7 days a week.

1.3.2. *Continuity*

Each SIRENE bureau shall build an internal structure, which guarantees the continuity of management, staff and technical infrastructure. Member States shall take appropriate measures to avoid loss of qualification and experience caused by staff turnover.

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.

1.3.3. *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 shall be carried out by each Schengen State. Recommendations and best practices laid down in the EU Schengen Catalogue: Schengen Information System, SIRENE, should be reflected in practice[18].

The specific features may differ as they shall answer to threats in the immediate surroundings and exact location of the SIRENE bureau. They may include, in particular:

— external windows fitted with security glass,

— secured and closed doors,

— brick/concrete walls enclosing the SIRENE bureau,

— closed-circuit television (CCTV), 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 have requisite access to documents from having to enter or to pass the SIRENE bureau offices, and/or

— sufficient back-up power and communication supply.

Security of the system

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

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.

1.3.4. *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.

1.3.5. *Communications*

Operational

The specific channel to use for SIRENE communications is the communication infrastructure for the Schengen environment (SISNET)[19]. Only if this channel is not available, shall another, and given the circumstances the most appropriate, means of communication 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 shall respect the instructions set out in Annex 5. The B[20], C[21] and D[22] 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. See also Section 2.16 on indication of urgency in SIRENE forms.

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 SISNET e-mail address for the exchange of non-operational information.

SIRENE Address Book (SAB)

The contact details of the SIRENE bureaux and relevant information for mutual communication and cooperation are collected and provided in the SIRENE Address Book (SAB). Each SIRENE bureau shall ensure that:

(a) information from the SAB is not disclosed to third parties;

(b) the SAB is known and used by the SIRENE operators;

(c) any update of the information listed in the SAB is provided without delay to the administrator of the SAB.

1.3.6. *Transliteration rules*

Transliteration rules, which can be found in Annex 2, shall be followed in the communication between SIRENE bureaux via SISNET.

1.3.7. *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 and capacity to perform this role, for which they are responsible pursuant to Article 92(4) and Article 108. It is therefore necessary to have a national data quality audit, including a review of the rate of alerts/hits and of data content.

National standards for training of end-users on data quality principles and practice should be established in cooperation with the national SIRENE bureau. 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.

1.3.8. *Structures*

All national agencies, including SIRENE bureaux, responsible for international police cooperation shall be organised in a structured fashion so as to prevent conflicts of competence and duplication of work.

1.3.9. *Archiving*

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

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

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

(d) In accordance with Article 112A of the Schengen Convention, personal data, held in files by the SIRENE Bureau as a result of exchanging information, shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest 1 year after the alert or alerts regarding the person or object concerned have been deleted from the SIS. However, data relating to a particular alert which a Member State has issued or to an alert in connection with which action has been taken on its territory may be stored for longer in accordance with national law.

(e) Supplementary information sent by the other Member States shall be stored according to national data protection legislation in the recipient Member State. The provisions of Title VI of the Schengen Convention, Framework Decision 2008/977/JHA and Directive 95/46/ECshall also apply, as appropriate.

(f) Information on misused identity shall be deleted after the deletion of the relevant alert.

1.4. **Staff**

1.4.1. *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 European 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 expertise can be provided by any personnel with the necessary legal background or experts from the judicial authorities.

The responsible national recruiting authorities shall take all the above skills and knowledge into consideration when recruiting new staff and, shall consequently, organise in-service training courses or sessions both at national and European 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. A low turnover of personnel is therefore propitious, which requires the unambiguous support of management to enable this devolved responsibility.

1.4.2. *Training*
National level

At national level, sufficient training shall ensure that staff meet the required standards laid down in this Manual[23].
European 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, to share information on national working methods and to create a consistent and equivalent level of knowledge. Furthermore, these will make staff aware of the importance of their work and the need for mutual solidarity in view of the common security of Member States.

1.4.3. *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.

1.5. **Technical infrastructure**

1.5.1. *SIRENE work-flow system*

Each SIRENE bureau shall have a computerised management system (work-flow system), which allows a great deal of automation in the management of the daily work-flow.

1.5.2. *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 additional action from the authority entering the alert.

1.5.3. *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.

1.5.4. *Data Exchange between SIRENE bureaux*

The instructions laid down for data exchange between SIRENE bureaux shall be respected[(24)].

1.5.5. *Data quality in the SIS*

In order to allow each SIRENE bureau to perform its role of data quality assurance coordinator (see paragraph 1.3.7 above), the necessary IT support should be available.

2. GENERAL PROCEDURES

The procedures described below are applicable to alerts issued under Articles 95 to 100 and the procedures specific for each Article can be found in the relevant specific section.

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

Several alerts may be issued by different Member States for the same subjects. It is essential that this does not cause confusion to end-users, and that they are clear as to the measures to 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. *Compatibility of alerts and order of priority*

Only one alert per Member State may be entered into the SIS for any one person or object.

Therefore, wherever possible and necessary, second and subsequent alerts on the same person or object shall be kept available at national level, so that they can be introduced when the first alert expires or is deleted.

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

Alerts for arrest (Article 95) are compatible with alerts for refusal of entry (Article 96), alerts on missing persons (Article 97) and alerts for a judicial procedure (Article 98). They are not compatible with alerts for discreet surveillance or specific checks (Article 99). In case of a hit on a person for whom an alert for arrest and an alert for refusal of entry have been entered, the procedures for arrest shall have priority over those for refusal of entry.

Alerts for refusal of entry are compatible with alerts for arrest. They are not compatible with alerts on missing persons, alerts for a judicial procedure or alerts for discreet surveillance or specific checks.

Alerts on missing persons are compatible with alerts for arrest and alerts for a judicial procedure. They are not compatible with alerts for refusal of entry and alerts for discreet surveillance or specific checks.

Alerts for a judicial procedure are compatible with alerts for arrest and alerts for missing persons. They are not compatible with alerts for refusal of entry and alerts for discreet surveillance or specific checks.

Alerts for discreet surveillance or specific checks are not compatible with alerts for arrest, alerts for refusal of entry, alerts on missing persons or alerts for a judicial procedure.

Within Article 99, alerts issued for **discreet surveillance** are incompatible with those for **specific checks**.

Different categories of alerts on objects are not compatible with each other (see the table on compatibility below).

The order of priority for alerts on persons shall be as follows:
— arrest with a view to surrender or extradition (Article 95),
— refusal of entry or stay in the Schengen territory (Article 96),
— placing under protection (Article 97),
— discreet surveillance (Article 99),
— specific checks (Article 99),
— communicating whereabouts (Articles 97 and 98).

The order of priority for alerts on objects shall be as follows:
— discreet surveillance (Article 99),
— specific check (Article 99),
— seizure or use as evidence (Article 100),

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

TABLE OF COMPATIBILITY OF ALERTS ON PERSONS

Order of importance	**Alert for arrest**	**Alert for refusal of entry**	**Alert on missing person (protection)**	**Alert for discreet surveillance**	**Alert for specific check**	**Alert on missing person (whereabouts)**	**Alert for judicial procedure**
Alert for arrest	yes	yes	yes	no	no	yes	yes

Alert for refusal of entry	yes	yes	no	no	no	no	no
Alert on missing person — protection	yes	no	yes	no	no	yes	yes
Alert for discreet surveillance	no	no	no	yes	no	no	no
Alert for specific check	no	no	no	no	yes	no	no
Alert on missing person — whereabouts	yes	no	yes	no	no	yes	yes
Alert for judicial procedure	yes	no	yes	no	no	yes	yes

TABLE OF COMPATIBILITY OF ALERTS ON OBJECTS

Order of importance	**Alert for discreet surveillance**	**Alert for specific check**	**Alert for seizure or use as evidence**
Alert for discreet surveillance	yes	no	no
Alert for specific check	no	yes	no
Alert for seizure or use as evidence	no	no	yes

2.1.2. *Checking for multiple alerts on a person*

To avoid entering incompatible multiple alerts, care shall 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 to this Manual.

The following procedure shall apply:

(a) if the processing of 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 which intends to enter a new alert shall contact the issuing SIRENE bureau to clarify whether the alert relates to the same person by means of an **L form**;

(c) if the check reveals that the details are identical and could relate to the same person, the SIRENE bureau which intends to enter a new alert 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.

2.1.3. *Negotiating the entry of a new alert if this is incompatible with an existing alert*

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 shall apply:

(a) if the alerts are compatible, the SIRENE bureaux do not need to consult each other; 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 using an **E form** so that ultimately only one alert is entered;

(c) alerts for arrest shall be entered immediately without awaiting the result of any consultation with other Member States;

(d) 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;

(e) if an alert is deleted, Member States who were not able to enter an alert are informed by the C.SIS. The SIRENE bureau should then 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 by him/her, 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 (action to be taken).

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

2.2.1. *Procedures following a hit*

The following procedures shall apply:

(a) one 'hit' on an individual or an object on which an alert has been issued shall usually be communicated by means of one **G form** to the SIRENE bureau of the issuing Member State;

(b) when notifying the issuing Member State of a hit, the applicable Article of the Schengen Convention shall, as appropriate, be indicated in field 090 of the **G form**, including additional information if necessary (e.g. 'MINOR').

(c) the **G form** shall provide as much as possible information on the hit, including on the action taken in field 088. Provision of supplementary information may be requested from the issuing Member State in field 089.

(d) if necessary the SIRENE bureau of the issuing Member State shall, following the hit, send any relevant specific information;

(e) the particular measures should be taken by the SIRENE bureau of the Member State that matched the alert to support the effective execution of the requested measures (action to be taken);

(f) if the SIRENE bureau of the Member State that achieved a hit intends to provide further information after a **G form** has been sent, it shall use an **M form**;

(g) if the hit concerns a person who is the subject of an alert under Article 95 or a minor who is the subject of an alert under Article 97, the SIRENE bureau of the Member State that matched the alert shall, where appropriate, inform the SIRENE bureau of the issuing Member State of the hit by telephone after sending a **G form**;

(h) 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 shall be informed in exceptional circumstances if supplementary information is required. For special procedures see Section 4.

2.2.2. *Communicating further information*

The following procedure shall apply:

(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) to the extent possible, and in accordance with the applicable rules of data protection, 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 medical information transmitted shall be kept only as long as is strictly necessary and shall be used exclusively for the purposes of medical treatment given to the person concerned.

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

If, following a hit, normal procedures cannot be executed, the exchange of data shall 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 the procedure to follow, in accordance with their national legislation and the provisions of the Schengen 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 order and safety, for serious reasons of national 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 shall 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 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.

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)**

Articles 106(2) and 106(3) 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 shall take place according to the following rule:

(a) 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**;

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

(c) if there is no agreement, the SIRENE bureau of the Member State that identified the error shall advise the authority responsible within its own country to refer 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 concerning him/herself and to request the correction of any errors. 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 by means of a **K form**.

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:

(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 to, or correction or deletion of 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 shall apply:

(a) the request for access, correction or deletion 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 by providing all the necessary information to answer the request;

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

(d) the Member State receiving an enquiry from an individual for access, correction or deletion shall take all the necessary measures to ensure a timely response.

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, correction or deletion, 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 shall apply:

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.

2.7. **Deletion of an alert when the conditions for maintaining it cease to be met**

The SIRENE bureau shall 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. The information from the **G form** provided by the SIRENE bureau of the Member State that has achieved a hit shall be provided by means of an **M form**.

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 maintaining the alert 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, in particular, 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 the alert into the SIS or modifying it.

If the code 3 is found in the field of 'category of identity' when the SIS is consulted, the official conducting the check shall 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.

Supplementary information on the person whose identity is misused may only be processed with his free and explicit consent for all items of information.

The person whose identity is misused shall, subject to his explicit consent and according to national procedures, provide the national SIRENE bureau of the issuing Member State with the information required to avoid the negative consequences of misidentification, such as genuine particulars, details of identity papers and/or by filling out the **Q form**.

Subject to the condition mentioned below, the photograph and the fingerprints of the person whose identity is misused may also be kept on file at the SIRENE bureau of the issuing Member State.

On the **Q form**, only the Schengen number refers to the data of the person sought by the SIS alert and all the other information relates to the victim of the misuse of identity. The information in heading 052 (Date document was issued) is compulsory. Heading 083 (Particular information concerning the alert) shall provide, as appropriate, further information on the case of misused identity (for example further distinguishing features) and shall always indicate the contact service which has further information on the alert.

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, including any fingerprints and photographs, 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 shall be deleted during the process of deleting the related alert.

2.9. Entering an alias

In order to avoid incompatible alerts of any category due to an alias to be entered, or to avoid problems for innocent victims, the SIRENE bureaux shall, if this information is available to them, inform each other about aliases and transmit all relevant information about the real identity of the subject sought. The Member State that entered the original alert is responsible for adding any aliases. If another Member State discovers an alias, it shall pass the matter on to the Member State that originally entered the alert.

2.10. SIRPIT (SIRENE Picture Transfer)

2.10.1. *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.

2.10.2. *Use of the data exchanged, including archiving*

Limitations on the use of data provided for in Articles 95 to 100 are set out in the Schengen Convention. Any use of pictures and fingerprints exchanged via SIRPIT, including archiving, shall comply with the relevant provisions of the Schengen Convention, applicable national provisions on data protection, in accordance with Directive 95/46/EC, Framework Decision 2008/977/JHA and the Convention 108 of the Council of Europe as appropriate.

2.10.3. *Technical requirements*

Every SIRENE bureau should fulfil the SIRPIT technical requirements.

The SIRENE bureau shall be able to, on the one hand, electronically exchange requests for comparison or verification and the results thereof and, on the other hand, send their requests electronically (without changes) to and receive results from their national identification service.

In SIRPIT, fingerprints and pictures are sent in an attachment on an input screen specially designed for this purpose.

2.10.4. *The national identification service*

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

2.10.5. *Use of the SIRENE **L form***

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

2.10.6. *SIRPIT procedure*

The SIRENE bureau of the country in which the person was discovered is known hereafter as ‘the discovering SIRENE’.

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:

2.10.6.1. 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.

2.10.6.2. 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 that 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.

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, in accordance with Article 112A of the Schengen Convention.

The fingerprints and pictures of a person not matching the data of the reported person which have been exchanged via SIRPIT shall be processed in accordance with the provisions of the Schengen Convention applicable national provisions on data protection in accordance with Directive 95/46/EC, Framework Decision 2008/977/JHA and Convention 108 of the Council of Europe, as appropriate.

2.10.6.3. Input screen

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

The input mask shall have the following data:

(1) Schengen ID number[(25)] (see note 1 below)

(2) Reference number[(25)] (see note 1 below)

(3) Date of fingerprints

(4) Place where fingerprints were taken

(5) Date of picture

(6) Reason for fingerprints (reason for the alert underlying the transmission of the fingerprints)

(7) Family name[(25)] (see note 2 below)

(8) First name[(25)] (see note 2 below)

(9) Maiden name

(10) Identity ascertained?

(11) Date of birth[(25)]

(12) Place of Birth

(13) Nationality

(14) Gender[(25)]

(15) Supplementary information
Remarks:
Notes:

(1) an entry shall be made in **either** Field 1 **or** Field 2

(2) the option '**unknown**' may be entered

When available, the place where and date on which the fingerprints were taken shall be entered.

2.11. Role of the SIRENE bureaux in police cooperation in the European Union

The exchange of supplementary information under the Schengen Convention shall not prejudice the tasks entrusted to the SIRENE bureaux in the area of international police cooperation by national law implementing other legal instruments of the European Union.

Additional tasks may be entrusted to the SIRENE bureaux, in particular, by the national law implementing Council Framework Decision 2006/960/JHA[(26)], Articles 39 and 46 of the Schengen Convention, in as far as they are not replaced by Framework Decision 2006/960/JHA, Articles 40 or 41 of the Schengen Convention or if the information falls within the scope of the mutual legal assistance.

If a SIRENE bureau receives a request falling outside its competence under national law, from another SIRENE bureau, it shall immediately forward it to the competent authority and inform the requesting SIRENE bureau about this action. If necessary, it shall provide support to the requesting SIRENE bureau to facilitate communication.

2.12. Relations between 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:

2.12.1. *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.

2.12.2. *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 also comply with this. 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 shall be consulted in advance. Such a change of channel is possible only in special cases.

2.12.3. *Use and distribution of Interpol diffusions and notices 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 insufficient information is available to enter an alert into the SIS). 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**'.

2.12.4. *Sending information to third countries*

As a general rule, data entered in the SIS shall not be made available to third countries. However, where a Member State has issued an alert, only the SIRENE bureau of that issuing Member State may decide whether to make available information to third countries (authorisation, diffusion means and channel). In so doing the SIRENE bureau shall observe the personal data protection provisions laid down in the Schengen Convention, Framework Decision 2008/977/JHA and Directive 95/46/EC, as appropriate. Use of the Interpol channel will depend on national provisions or procedures.

2.12.5. *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.

2.12.6. *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.

2.13. **Cooperation with EUROPOL and EUROJUST**

In order to streamline cooperation between SIRENE bureaux, appropriate national procedures shall be established, in particular for cases where EUROPOL or EUROJUST accesses the SIS and achieves a hit.

2.14. **Special types of search**

2.14.1. *Geographically targeted search*

A geographically targeted search is a search carried out when the 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 shall be sent at time of creation of the alert or the obtaining of the information on whereabouts, shall include information on the 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 and Article 9(3) of the Framework Decision on EAW).

Such an alert increases the chances of success, if the person or object moves unexpectedly from one place to another within the Schengen area. Cases where no alert is created shall be restricted to special circumstances, in particular if there is no sufficient information available to create an alert.

2.14.2. *Search with participation of special police units for targeted search (FAST)*

The services provided by special units that conduct targeted searches (FAST) shall also be used in suitable cases by SIRENE bureaux in the requested Member States. The alert in SIS cannot

be replaced by international cooperation of the above mentioned police units. Such cooperation shall not overlap the SIRENE bureau's role as a focal point for searches using the SIS.

Cooperation, as appropriate, shall be established to ensure that the SIRENE bureau of the issuing Member State is informed by their national FAST about any ongoing operation relating to an alert entered in the SIS. Where appropriate this SIRENE bureau shall provide this information to other SIRENE bureaux.

The SIRENE bureaux shall ensure fast flow of supplementary information, including information on a hit, to the national FAST if the latter is involved in the search.

2.15. **Flagging**

A flag shall be added at the request of another Member State.

Articles 94(4), 95(3), 97 and 99(6) of the Schengen Convention allow a Member State to refuse to perform a requested action on its territory at any time by requesting that a flag be added to the alerts in accordance with Articles 95, 97 or 99 where it considers that an alert is incompatible with its national law, its international obligations or essential national interests. The reasons for the request shall be provided simultaneously.

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 only for Article 95 alerts. Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

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

The following procedure shall apply:

(a) if a Member State requires a flag to be added it shall request, via its SIRENE Bureau, the flag from the issuing Member State by means of an **F form**, using fields 071-074[(27)]. For more details concerning the national law field 080 and, where appropriate, for supplementary information explaining the reason for the flag and other supplementary information concerning the alert, field 083 shall be used;

(b) the Member State that issued the alert shall add the requested flag immediately;

(c) once information has been exchanged, based on the information provided for in the consultation process by the Member State requesting the flag, the alert may need to be amended or deleted or the request may be withdrawn.

2.15.2. *A request for deletion of a flag*

Member States shall request the deletion of the previously requested flag as soon as the reason for the flag is no longer valid. This may be the case, in particular, if the national legislation has changed or if further information exchange about the case revealed that the circumstances mentioned in Articles 94(4), 95(3), 97 and 99(6) of the Schengen Convention no longer exist.

The following procedure shall apply:

(a) the SIRENE bureau which previously requested the flag to be added shall request the SIRENE bureau of the Member State that issued the alert to delete the flag. This request shall be made by means of an **F form**. Field 075 shall be used for this purpose[(28)]. For more details concerning the national law field 080 shall be used and, where appropriate, for supplementary information explaining the reason for the deletion of the flag and for other supplementary information concerning the alert field, 083 shall be used;

(b) the SIRENE bureau of the Member State that issued the alert shall delete the flag immediately.

2.16. Indication of urgency in SIRENE forms

SIRENE forms to be dealt with by the requested SIRENE bureau with highest priority may be marked 'URGENT', followed by the reason for urgency. Field 083 in the SIRENE forms shall include this information as the first piece of information, where appropriate.

3. ALERTS PURSUANT TO ARTICLE 95[29]

The following steps shall 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,
— deletion of an alert,
— misused identity.

3.1. Member State checks prior to issuing the alert

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

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

Sufficient detail to enable other SIRENE bureaux to verify the alert should be contained in the EAW/extradition request 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').

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 shall apply:

(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 under Article 95(2), second sentence, 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 in the system per wanted person. A check is therefore 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. On the basis of this alert, only one **A form** shall be sent to Member States in accordance with the procedure referred to in Section 3.4. Alternatively, a single EAW could be issued to cover all offences.

For general procedures on checking multiple alerts see Section 2.1.2.

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 issued 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. If the alerts are compatible, **G forms** shall be sent, in the event of a hit, in response to all requests.

3.3.2. *Exchange of information*

See general procedures in Section 2.1.2 and 2.1.3.

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, shall be used and the information contained in these forms shall 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 the non-execution of such a 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 the non-execution of such a 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 the non-execution of such a 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 the non-execution of such a 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 in which 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 field 083 of an **M form**:

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

  (a) to indicate 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 rendered in absentia. If this is not the case, mention the legal safeguards. From the date of application of Framework Decision 2009/299/JHA[(30)], the conditions of the decision rendered in absentia shall be indicated in field 083 as specified in the EAW. Codes 2, 3.1a, 3.1b, 3.2, 3.3 (decision not contested), 3.3 (no request for retrial or appeal) and 3.4 shall be referred to and, where applicable, information shall be provided about how the relevant condition has been met,
— 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 3 years, as defined by the laws of the issuing Member State, according to Article 2(2) of the Framework decision (or Section [(e)I] 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) shall 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 12 months;

(b) or, where a sentence has been passed or a detention order has been made, that the sentence is of at least 4 months.

— If 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.

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 ref. 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.

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. *Entering an alias*

See general procedures in Section 2.9.

In case of alerts for arrest, the SIRENE Bureau shall use field 011 of the **A form**[31] (at the time of entry of the alert) or subsequently the **M form**, when informing the other Member States of aliases regarding an alert issued pursuant to Article 95, if this information is available to the SIRENE bureau.

3.4.4. *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 reference number, issuing date, place and authority as well as the expiry date of the passport or identity document,
— description of the person sought,
— surname and given name of the wanted person's mother and father,
— to check whether a photo and/or finger prints are available,
— last known address.

As far as is possible, this information, including any photographs and fingerprints, 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 similar to those of the person on whom an alert has been issued.

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

The information mentioned in 3.3.1 and 3.3.2 shall 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 **M forms** describing different EAWs (or extradition requests) can be sent if necessary. The **M form** shall contain information in particular on the type of offence on which the EAW is based, the date of the commission of the offence and the statute of limitations. If the issue of a new EAW concerning a person already subject of a EAW requires the replacement of an existing **A form**, the fact that the new **A form** is a replacement shall be indicated on the new form in field 030.

3.5. **Flagging**

For general procedures see Section 2.15.

A flagged alert shall be regarded as being issued for the purposes of communicating the place of residence of the person concerned.

3.5.1. *Systematic request for a flag to be added to alerts on persons wanted for arrest for extradition purposes where Council Framework Decision 2002/584/JHA of 13 June*

2002 on the European arrest warrant and the surrender procedures between Member States[32] *does not apply*

The following procedure shall apply:

(a) in the case of alerts on persons wanted for arrest for extradition purposes, where Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States does not apply, a SIRENE bureau may ask other SIRENE bureaux to add a flag systematically to Article 95 alerts issued on its nationals;

(b) any SIRENE bureau wishing to do so shall send a written request to other SIRENE bureaux;

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

(d) the flag shall remain until the requesting SIRENE bureau asks for its cancellation.

If the circumstances mentioned in Article 94(4) of the Schengen Convention no longer exist, the Member State that requested the flag shall 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** shall be forwarded to the authority of the Member State which executes the EAW. If the original EAW is requested, it shall be sent by the issuing judicial authority directly 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*

For the general procedure see Section 2.2.1.

In addition, the following procedure shall apply:

(a) a hit on an individual on which an Article 95 alert has been issued shall always be communicated to the SIRENE bureau of the issuing Member State. Moreover, after sending the **G form**, the hit shall also be communicated, where appropriate, by telephone;

(b) the authority competent for receiving the EAW or extradition request, its full communication contacts (postal address, phone and, if available, fax and e-mail), reference number (if available), competent person (if available), requested language, time limit for and form of delivery shall be provided in field 091 of the **G form**;

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

(d) 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 SIRENE bureaux may transmit further information on Article 95 alerts, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance.

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 shall be informed of the hit and its outcome.

This procedure has technical implications as the alert may need to be deleted and another alert which had previously been excluded from the SIS can now be entered.

3.7.4. *Supplementary information exchange about surrender or extradition*

Information, when provided by the competent judicial authorities to the SIRENE bureau on whether the surrender or extradition may take place of a person for whom an alert for arrest has been issued, shall immediately be provided to the SIRENE bureau of the Member State issuing the alert by means of an **M form**, marked in field 083 with the word 'SURRENDER' or 'EXTRADITION'[(33)]. The modalities of the surrender or extradition should be communicated via the SIRENE bureaux as soon as possible.

If the transit of a wanted person is necessary, the SIRENE bureau of the Member State to be transited shall provide the necessary support and assistance, in response to a request by the SIRENE bureau or the competent judicial authority of the issuing Member State, sent by the SIRENE bureau, by means of an **M form**.

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 by the C.SIS (once the expiry date has passed) or by the service that entered the alert in the SIS (once the conditions for maintaining the alert 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.

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**

See general procedure in Section 2.8.

4. ALERTS PURSUANT TO ARTICLE 96[34]

The following steps shall be followed:

— entry of the alert,
— check for multiple alerts, reference is made to General Procedures in Section 2.1,
— entering an alias, reference is made to General Procedures in Section 2.9,
— misused identity, reference is made to General Procedures in Section 2.8,
— SIRPIT procedure, reference is made to General Procedures in Section 2.10,
— general and special procedures to be followed.

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 individual is already on the territory of the Member State, it allows national authorities to take the appropriate action for issuing residence permits, long-stay visas or expulsion.

Carrying out the information procedures laid down under Article 5(4) of the Schengen Borders Code and the consultation procedures laid down under Article 25 of the Schengen Convention, falls within the competences of the authorities responsible for border controls and issuing residence permits or visas. In principle, the SIRENE bureaux shall be involved in these procedures only in order to transmit supplementary information directly related to the alerts (e.g. notification of a hit, clarification of identity) or to erase alerts.

However, the SIRENE bureaux may also be involved in transmitting supplementary information necessary for the expulsion of, or for refusing entry to, a third-country national; and, may be involved in transmitting any supplementary information further generated by these actions.

4.2. Entry of alerts pursuant to Article 96

Enter the alert into the SIS, if the SIRENE bureau is the authority designated for such entries.

In the exceptional case of entry of an alert on a third-country national enjoying the right of free movement, the SIRENE bureau of the Member State issuing the alert shall send an **M form** to all the other Member States, based on the information provided by the authority that has entered the alert[35].

4.3. Entering an alias

See general procedure in Section 2.9.

4.4. Misused Identity

If 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.

For gathering and communicating information on a person whose identity is misused, see general procedure in Section 2.8.

4.5. Types of SIRENE procedures to be followed

The following *general procedures* shall apply, to the SIRENE bureaux, to the extent that they forward supplementary information:

(a) exchange of information when refusing entry or expelling from the Schengen territory;

(b) exchange of information when issuing residence permits or long-stay visas.

The following *special procedures* shall apply to the SIRENE bureaux to the extent that they forward supplementary information:

(a) special procedures as provided for in Article 25 of the Schengen Convention;

(b) special procedures as provided for Article 5(4) of the Schengen Borders Code;

(c) exchange of information on a third-country national who is a beneficiary of the right of free movement;

(d) deletion of alerts entered for EU citizens.

4.6. **Exchange of information following a hit**

4.6.1. *Exchange of information when refusing entry or expelling from the Schengen territory*

The following procedure shall apply:

(a) a Member State may ask to be informed of any hits on alerts for refusal of entry or stay that it has issued. Any Member State that wishes to take up this option shall ask the other Member States in writing;

(b) the executing Member State may take the initiative and inform the issuing Member State that the alert has been matched and that the third-country national has not been granted entry or has been expelled from the Schengen territory;

(c) If, on its territory, a Member State intercepts a third-country national for whom an alert has been issued, the issuing Member State, upon request, shall forward the information required to return the person concerned. Depending on the needs of the executing Member State and, if available at the issuing Member State, this information, given in an **M form**, shall include the following:
— the type and reason for the decision,
— the authority issuing the decision,
— the date of the decision,
— the date of service (the date on which the decision was served),
— 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 out in the Schengen Borders Code, and by the issuing Member State, shall be followed.

There might also be an urgent need for supplementary information to be exchanged via the SIRENE bureaux in specific cases in order to identify an individual with certainty.

4.6.2. *Exchange of information when issuing residence permits or visas*

The following procedure shall apply:

(a) the executing Member State may inform the Member State which issued an alert for refusal of entry or stay that the alert has been matched in the course of the procedure for issuing a residence permit or a long-stay visa;

(b) the Member State that issued the alert may then inform other Member States using an **M form**, if appropriate;

(c) if so requested, in accordance with national legislation, the SIRENE bureaux of the Member States concerned may assist in transmitting the necessary information to the appropriate authorities responsible for issuing residence permits and visas.

4.6.3. *Special procedures as provided for in Article 25 of the Schengen Convention*

4.6.3.1. Procedure under Article 25(1) of the Schengen Convention

If a Member State that is considering granting a residence permit or long-stay visa discovers that the applicant concerned is the subject of an alert for refusal of entry or stay issued by another Member State, it shall consult with the Member State that issued the alert via the SIRENE bureaux. An **N form** shall be used for that purpose. The alert shall be deleted if, after consultation, the Member State maintains its decision to issue the residence permit. The person can, nevertheless, be put on a Member State's national list of alerts for refusal of entry.

4.6.3.2. Procedure under Article 25(2) of the Schengen Convention

If a Member State that entered an alert for refusal of entry or stay finds out that the person who is the subject of the alert has been issued a residence permit or long-stay visa, it shall instigate a consultation procedure with the Member State that issued the residence permit or long-stay visa, via the SIRENE Bureaux using an **O form**. The consultation via SIRENE bureaux using an **O form** shall also take place if the Member State that issued the residence permit or long-stay visa discovers later that there is an alert for refusal of entry or stay in the SIS on that person[(36)].

If a third Member State (i.e. neither the one which granted the residence permit or long-stay visa nor the one which issued the alert) discovers that there is an alert on a third-country national that holds a residence permit or long-stay visa from one of the Member States, it shall notify both the Member State which granted the permit or long-stay visa and the Member State which issued the alert, via SIRENE bureaux using an **H form**.

If the procedure foreseen under Article 25 of the Schengen Convention entails deleting an alert for refusal of entry or stay, the SIRENE bureaux shall, whilst respecting their national legislation, offer their support if so requested.

4.6.4. *Special procedures as provided for in Article 5(4) of the Schengen Borders Code*

4.6.4.1. Procedure in cases falling under Article 5(4)(a) of the Schengen Borders Code

According to Article 5(4)(a) of the Schengen Borders Code, a third-country national who is subject to an alert for refusal of entry or stay and, at the same time, has a **residence permit, long-stay visa** or a **re-entry visa** issued by one of the Member States, shall be allowed entry for transit purposes to the Member State which issued the residence permit, long-stay visa or re-entry visa, when crossing a border in another Member State. The entry may be refused if this Member State has issued a national alert for refusal of entry.

If the third-country national concerned tries to enter the Member State which has entered the alert into the SIS, his/her entry may be refused by this Member State. However, at the request of the competent authority, the SIRENE bureau of that Member State shall consult the SIRENE bureau of the Member State that issued the residence permit using an **O form** in order to allow the competent authority to determine whether there are sufficient reasons for withdrawing the residence permit. If the residence permit is not withdrawn, the alert in the SIS shall be deleted but the person concerned may nevertheless be put on the national list of alerts for refusal of entry.

If this person tries to enter the Member State that issued the residence permit, he/she shall be allowed entry into the territory but the SIRENE bureau of that Member State, at the request of the competent authority, shall send an **O form** to the SIRENE bureau of the Member State that

issued the alert in order to enable the competent authorities concerned to decide on withdrawal of the residence permit or long-stay visa or deletion of the alert.

If the third-country national concerned tries to enter a third Member State, which is neither the State that issued the alert nor the one which granted the residence permit or long-stay visa, and the third Member State finds out that there is an alert in the SIS on that person, although he/she has a residence permit or long-stay visa issued by one of the Member States, it shall allow transit towards the Member State that issued the residence permit or long-stay visa. The entry may be refused if this third Member State has put the person concerned on its national list of alerts. In both cases, at the request of the competent authority, its SIRENE bureau shall send the SIRENE Bureaux of the two Member States in question an **H form** informing them of the contradiction and requesting that they consult each other in order to either delete the alert in the SIS or to withdraw the residence permit or long-stay visa. It may also request to be informed of the result of any consultation.

4.6.4.2. Procedure in cases falling under Article 5(4)(c) of the Schengen Borders Code

According to Article 5(4)(c) a Member State may derogate from the principle that a person for whom an alert for refusal of entry was issued shall be refused entry on humanitarian grounds, on grounds of national interest or because of international obligations. At the request of the competent authority, the SIRENE bureau of the Member State that allowed entry shall inform the SIRENE bureau of the issuing Member State thereof using an **H form**.

4.7. Exchange of information on a third-country national who is a beneficiary of the right of free movement

Concerning a third-country national who is a beneficiary of the right of free movement within the meaning of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, special rules shall apply[37].

4.7.1. *Exchange of information following a hit*

If there is a hit on a third-country national who is a beneficiary of the right of free movement, the following procedure shall be followed:

(a) at the request of the competent authority, the SIRENE bureau of the executing Member State shall immediately contact the SIRENE bureau of the issuing Member State using a **G form**, in order to obtain the information necessary to decide without delay on the action to be taken;

(b) upon receipt of a request for information, the SIRENE bureau of the issuing Member State shall immediately start gathering the required information and send it as soon as possible to the SIRENE bureau of the executing Member State;

(c) the SIRENE bureau of the issuing Member State shall check with the competent authority, if this information is not yet available, whether the alert may be kept in accordance with Directive 2004/38/EC. If the competent authority decides to keep the alert, the SIRENE Bureau of the Member State issuing the alert shall inform all the other SIRENE bureaux thereof, by means of an **M form**;

(d) the executing Member State shall inform via its SIRENE bureau the SIRENE bureau of the issuing Member State whether the requested action was carried out (confirming this by using an **M form**) or not (using an **H form**).

4.7.2. *Exchange of information if, in the absence of a hit, a Member State discovers that there is an alert for refusal of entry for a third-country national who is a beneficiary of the right of free movement*

If, in the absence a hit, a Member State discovers that there is an alert for refusal of entry for a third-country national who is a beneficiary of the right of free movement, the SIRENE bureau of this Member State shall, at the request of the competent authority, send an **M form** to the SIRENE bureau of the issuing Member State informing it about this.

The SIRENE bureau of the issuing Member State shall check with the competent authority, if this information is not yet available, whether the alert may be kept in accordance with Directive 2004/38/EC. If the competent authority decides to keep the alert, the SIRENE Bureau of the Member State issuing the alert shall inform all the other SIRENE bureaux thereof, by means of an **M form**.

4.8. **Deletion of alerts entered for EU citizens**

When a third-country national for whom an alert for refusal of entry or stay has been issued, acquires citizenship of one of the Member States[38], the alert shall be deleted. If the change of citizenship comes to the attention of a SIRENE bureau of a country other than the issuing one, the former shall send the SIRENE bureau of the issuing Member State a **J form**, in accordance with the procedure for rectification and deletion of data found to be legally or factually inaccurate (see Section 2.5).

4.9. **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 shall be informed in exceptional circumstances if supplementary information is required in accordance with Sections 4.6 to 4.8. (See also Section 2.2.1 (g)).

However, SIRENE bureaux shall provide statistics on those hits.

5. ALERTS PURSUANT TO ARTICLE 97[39]

The following steps have to be considered:

— check for multiple alerts, reference is made to General Procedures Section 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 Section 2.8,
— SIRPIT procedure, reference is made to the General Procedures Section 2.10,

5.1. **Flagging**

See general procedures in Section 2.15.

5.2. **Provision of descriptive detail on missing minors and other persons assessed as being at risk**

SIRENE bureaux shall have ready access to all relevant supplementary information at national level regarding missing person alerts in order for the SIRENE bureaux to be able to play a full role in reaching a successful outcome to cases, facilitating identification of the person and providing supplementary information promptly on matters linked to the case. Relevant supplementary information may cover, in particular, national decisions on the custody of a child or vulnerable person or requests for the use of ‘Child Alert’ mechanisms.

In the case of a high-risk missing person, field 083 of the **M form** should begin with the word 'urgent'. This urgency should be reinforced by a telephone call highlighting the importance of the **M form** and its urgent nature.

As field 083 of the **M form** has limited technical capacity for holding information, a common method for entering structured supplementary information and the order of that information shall be used[40].

As not all vulnerable missing persons will cross national borders, decisions on the provision of supplementary information (on descriptive detail) and its recipients shall be taken on a case-by-case basis, covering the entire range of circumstances. Following a decision at national level on the extent of forwarding required for such supplementary information, the SIRENE bureau shall, as far as is appropriate, take one of the following measures:

(a) retain the information in order to be able to forward supplementary information upon the request of another Member State;

(b) forward the **M form** to the competent SIRENE bureau if enquiries indicate a likely destination for the missing person;

(c) forward the **M form** to all the competent SIRENE bureaux, based on the disappearance circumstances for the purpose of supplying all data concerning the person in a short period of time.

Once information has been received by a SIRENE bureau, it shall, in order to maximise the opportunities for locating the person in a targeted and reasoned fashion, be communicated, as far as is appropriate, to:

(a) relevant border posts;

(b) the competent administrative and police authorities for the location and protection of persons;

(c) the relevant consular authorities of the Member State which has entered the alert, after a hit is found in the SIS.

5.3. **After a hit**

For general procedures see Section 2.2.

When a hit is achieved on a missing person who is of age, the SIRENE bureau of the Member State achieving a hit shall advise the end-user that the communication of data on a missing person who is of age shall be subject to the person's consent[41]. The consent shall be in writing or at least a written record shall be available. In cases where consent is refused, this shall be in writing or recorded officially. For communicating further information see procedure in Section 2.2.2.

6. ALERTS PURSUANT TO ARTICLE 98[42]

The following steps have to be considered:

— Check for multiple alerts, reference is made to General Procedures Section 2.1,
— enter the alert into the SIS,
— the exchange of information after a hit,
— misused identity, reference is made to General Procedures Section 2.8,
— SIRPIT procedure, reference is made to the General Procedures Section 2.10,

6.1. **After a hit**

For general procedures see Section 2.2.

In addition, the following rules shall apply:

(a) the place of residence or domicile shall be obtained using all measures allowed by the national legislation of the Member State where the person was located;

(b) national procedures shall be in place, as appropriate, to ensure that alerts are only kept in the SIS for the time required to meet the purposes for which they were supplied.

The SIRENE bureaux may transmit further information on Article 98 alerts, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance.

7. ALERTS PURSUANT TO ARTICLE 99[43]

The following steps have to be considered:

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

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

— the exchange of information after a hit,

— SIRPIT procedure, reference is made to General Procedures Section 2.10.

7.1. Entering an alias

See general procedure in Section 2.9.

Inform the other Member States of aliases regarding an alert issued pursuant to Article 99 by means of an **M form**. Whenever needed, the SIRENE bureaux shall transmit this information to their national authorities responsible for each category of alert.

7.2. Informing other Member States when issuing alerts requested by authorities responsible for national security

When entering an alert at the request of an authority responsible for national security, the SIRENE bureau of the issuing Member State shall inform all the other SIRENE bureaux about it by using an **M form** and indicating Article 99(3) in field 083.

The confidentiality of certain information shall be safeguarded in accordance with national law, including keeping contact between the SIRENE bureaux separate from any contact between the services responsible for national security.

7.3. Flagging

See general procedure in Section 2.15.

7.4. Communicating further information following a hit

For Article 99(2) alerts see general procedure in Section 2.2.

In addition, the following procedure shall apply:

(a) when a positive hit occurs on an Article 99(3) alert, the discovering SIRENE bureau shall inform the requesting SIRENE bureau of the results (discreet surveillance or specific check) via the **G form**. At the same time the discovering SIRENE bureau shall inform its own competent service responsible for national security;

(b) if the national security service in the discovering Member State decides that the alert requires a validity flag, it shall contact its national SIRENE bureau in order to create

the flag with the requesting SIRENE bureau (via the **F form**). It shall not be required to explain the reasons for the flag, but the request shall be made through SIRENE channels;

(c) a specific procedure is required to safeguard the confidentiality of information. Therefore, any contact between the services responsible for national security shall be kept separate from the contact between the SIRENE bureaux. Consequently, the reasons for requesting a flag shall be discussed directly between national security services and not through SIRENE bureaux.

8. ALERTS PURSUANT TO ARTICLE 100[44]

The following steps shall be considered:

— check for multiple alerts,

— the exchange of information after a hit,

— SIRPIT procedure, reference is made to General Procedures Section 2.10.

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 vehicle identification number (VIN).

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. 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 to this Manual.

The consultation procedures to be applied by the SIRENE bureaux for vehicles shall be the same as for persons. For general procedures see Section 2.1.

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.

8.1.2. *VIN Twins*

VIN twin refers to a vehicle of the same type with the same vehicle identification number (VIN) as a vehicle entered in the SIS (e.g. a tractor and a motorcycle with the same VIN do not fall into this category). The following specific rules shall apply to avoid the negative consequences of a repeated seizure of the legally registered vehicle with the same VIN.

The following procedure shall apply:

(1) where the possibility of a VIN twin is established, the SIRENE bureau shall, as appropriate:

(a) ensure that there is no error in the SIS alert and the alert information is as complete as possible;

(b) check the circumstances of the case giving rise to an alert in the SIS;

(c) find out the history of both vehicles from their production;

(d) request a thorough check of the seized vehicle, in particular its VIN, to verify whether it is the legally registered vehicle.

The SIRENE bureaux involved shall closely cooperate in taking such measures.

(2) where the existence of a VIN twin is confirmed, supplementary information provided by the Member State creating the original alert, by means of the **M form**, shall include, as appropriate, the marks describing the legally registered vehicle and distinguishing it from the vehicle entered in the SIS[(45)];

(3) furthermore, on becoming aware of a case of a VIN twin, the issuing Member State shall check whether it is necessary to maintain the alert in the SIS.

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

The SIRENE bureaux may transmit further information on alerts entered under Article 100, and in so doing may act on behalf of judicial authorities, if this information falls within the scope of mutual judicial assistance.

The SIRENE bureau of the issuing Member State shall send the requested further information as quickly and comprehensively as possible via a **P form**, in response to a **G form** when a hit is obtained 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 shall provide hit, communication and workload statistics. The statistics shall cover all the Articles and all types of alerts. The statistics report shall be sent electronically to the General Secretariat of the Council.

(**1**) OJ L 239, 22.9.2000, p. 19.

(**2**) Decision of the Executive Committee of 22 December 1994 on bringing into force the Implementing Convention (SCH/Com-ex (94)29 rev. 2. (OJ L 239, 22.9.2000, p. 130).

(**3**) Decisions of the Executive Committee of 7 October 1997 (SCH/com-ex 97(27) rev. 4) for Italy and (SCH/com-ex 97(28) rev. 4) for Austria.

(**4**) Council Decision 1999/848/EC of 13 December 1999 on the full application of the Schengen *acquis* in Greece (OJ L 327, 21.12.1999, p. 58).

(**5**) Council Decision 2000/777/EC of 1 December 2000 on the application of the Schengen *acquis* in Denmark, Finland and Sweden, and in Iceland and Norway (OJ L 309, 9.12.2000, p. 24).

(**6**) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provision of the Schengen *Acquis* (OJ L 131, 1.6.2000, p. 43).

(**7**) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provision of the Schengen *Acquis* (OJ L 64, 7.3.2002, p. 20).

(**8**) Council Decision 2004/926/EC of 22 December 2004 on putting into effect of parts of the Schengen *acquis* by the United Kingdom of Great Britain and Northern Ireland (OJ L 395, 31.12.2004, p. 70).

(**9**) OJ C 340, 10.11.1997, p. 92.

(**10**) OJ L 323, 8.12.2007, p. 34.

(**11**) OJ L 166, 1.7.2010, p. 17.

(**12**) OJ L 53, 27.2.2008, p. 52.

(**13**) OJ L 327, 5.12.2008, p. 15.

(**14**) OJ L 83, 26.3.2008, p. 3.

(**15**) See footnote 1.

(**16**) As set out in Articles 101A and 101B of the Schengen Convention.

(**17**) 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 Council Decision 2005/211/JHA (OJ L 68, 15.3.2005, p. 44).

(**18**) Detailed guidance on IT security measures is provided in Section 5 of the revised EU Schengen Catalogue: Schengen Information System, SIRENE.

(**19**) See Council Decision 2000/265/EC of 27 March 2000 on the establishment of a financial regulation governing the budgetary aspects of the management by the Deputy Secretary-General of the Council, of contracts concluded in his name, on behalf of certain Member States, relating to the installation and the functioning of the communication infrastructure for the Schengen environment, 'SISNET' (OJ L 85, 6.4.2000, p. 12).

(**20**) Information further to an alert regarding national security.

(**21**) Checking for a double alert on the same person.

(**22**) Checking for a double alert on the same vehicle.

(**23**) Staff shall receive, among other subjects, appropriate training about data security and data protection rules and shall be informed of any relevant criminal penalties. Staff shall also be aware of the relevant national rules of professional secrecy or other equivalent obligations of confidentiality which shall apply to all SIRENE personnel.

(**24**) Council Document 5076/07, version 5.6

(**25**) Mandatory

(**26**) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).

(**27**) For the technical implementation see the Data Exchange between SIRENEs document referred to in Section 1.5.4.

(**28**) See footnote 26.

(**29**) 'Persons wanted for arrest for surrender/extradition'

(**30**) Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ L 81, 27.3.2009, p. 24).

(**31**) See footnote 26.

(**32**) OJ L 190, 18.7.2002, p. 1.

(**33**) See also Section 2.16. on indication of urgency in SIRENE forms.

(**34**) Third-country nationals for whom an alert has been issued for the purposes of refusing entry (Articles 25 and 96 of the Schengen Convention).

(**35**) According to Directive 2004/38/EC, a person benefiting from the right of free movement may only be refused entry or stay on the grounds of public policy or public security when their personal conduct represents a genuine, immediate, and sufficiently serious threat affecting one of the fundamental interests of society and when the other criteria laid down in Article 27(2) of this Directive are respected. Article 27(2) stipulates: 'Measures taken on grounds of public policy or public security shall comply with the principle of proportionality and shall be based exclusively on the personal conduct of the individual concerned. Previous criminal convictions shall not in themselves constitute grounds for taking such measures. The personal conduct of the individual concerned must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society. Justifications that are isolated from the particulars of the case or that rely on considerations of general prevention shall not be accepted.' Moreover, there are additional limitations for persons enjoying the right of permanent residence who can only be refused entry or stay on **serious** grounds of public policy or public security as stated in Article 28(2) of the Directive.

(**36**) In the case of alerts for refusal of entry issued for the family members of EU citizens, it is necessary to recall that it is not possible as a matter of routine to consult SIS prior to issuing a residence card for such a person. Article 10 of the Directive 2004/38/EC lists the necessary conditions for acquiring right of residence for more than 3 months in a host Member State by family members of Union citizens who are third-country nationals. This list, which is exhaustive, does not allow for routine consultation of the SIS prior to the issuing of residence cards. Article 27(3) of this Directive specifies that Member States may request, should they consider it essential, information from other MS only regarding any previous police record (so, i.e. not all of the SIS data). Such enquiries shall not be made as a matter of routine.

(**37**) See footnote 34.

(**38**) Citizens of Iceland, Liechtenstein, Norway and Switzerland enjoy the right of free movement equivalent to those of citizens of the European Union under agreements between the Community and its Member States, on the one hand, and these countries, on the other.

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

(**40**) Data of disappearance:

(a) Place, date and time of the disappearance.
(b) Circumstances of disappearance.

Details of the missing person:

(c) Apparent age.
(d) Height.
(e) Skin colour.
(f) Colour and shape of hair.
(g) Colour of eyes.
(h) Other physical details (i.e. piercings, deformations, amputations, tattoos, marks, scars, etc.).
(i) Psychological particulars: at risk of suicide, mental illness, aggressive behaviour, etc.
(j) Other details: necessary medical treatment, etc.
(k) Clothes worn at the time of the disappearance.

(l) Photograph: available or not.
(m) Ante-mortem form: available or not.
Related information:
(n) Person/s who could accompany him or her (and Schengen ID if available).
(o) Vehicle/s relating to the case (and Schengen ID if available).
The titles of the different sub fields themselves are not to be included as part of field 83, but just the reference letter.

(**41**) For clarity on consent in matters of on the protection of individuals with regard to the processing of personal data and on the free movement of such data see Article 2(h) Directive 95/46/EC of the European Parliament and of the Council (OJ L 281, 22.11.1995, p. 31).

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

(**43**) Persons or vehicles for the purpose of discreet surveillance or of other specific checks.

(**44**) Objects sought for the purpose of seizure or use as evidence in criminal proceedings.

(**45**) Such supplementary may include:
(a) Vehicle number plate details
(b) Category of vehicle, make of vehicle, model of vehicle, colour
(c) Other easily recognisable distinguishing features or details
(d) Full details of the owner
(e) Serial number of vehicle registration document.