ANNEX

SIRENE Manual and other implementing measures[(1)]

2. GENERAL PROCEDURES

The procedures described below are applicable to all categories of alerts, and the procedures specific to each category of alert can be found in the relevant parts of this Manual.

2.1. Definitions

'Issuing Member State'	Member State that entered the alert into the SIS II;
'Executing Member State'	Member State that executes the action to be taken following a hit;
'Hit'	when an end-user conducts a search in the SIS II and finds out that an alert exists which matches the details entered, and further action needs to be taken;
'Flag'	suspension of validity that may be added to alerts for arrest, alerts on missing persons and alerts for checks, where a Member State considers that to give effect to an alert is incompatible with its national law, its international obligations or essential national interests. When the alert is flagged, the requested action to be taken on the basis of the alert shall not be taken on the territory of this Member State.

2.2. Multiple Alerts (Article 34(6) of the SIS II Regulation and 49(6) of the SIS II Decision)

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

This calls for:

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

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

2.2.1. Compatibility of alerts and order of priority

Only one alert per Member State may be entered into the SIS II 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 26 of the SIS II Decision) are compatible with alerts for refusal of entry (Article 24 of the SIS II Regulation), alerts on missing persons (Article 32 of the SIS II Decision) and alerts for a judicial procedure (Article 34 of the SIS II Decision). They are not compatible with alerts for checks (Article 36 of the SIS II Decision).

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

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 checks.

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

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

Within alerts for checks, alerts issued for '**discreet checks**' 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 26 of the SIS II Decision),
— refusing entry or stay in the Schengen territory (Article 24 of the SIS II Regulation),
— placing under protection (Article 32 of the SIS II Decision),
— specific checks (Article 36 of the SIS II Decision),
— discreet checks (Article 36 of the SIS II Decision),
— communicating whereabouts (Articles 32 and 34 of the Decision).

The order of priority for alerts on objects shall be as follows:
— use as evidence (Article 38 of Decision),
— seizure (Article 38 of Decision),
— specific check (Article 36 of Decision),
— discreet check (Article 36 of Decision).

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 specific check**	**Alert for discreet 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 specific check	no	no	no	yes	no	no	no
Alert for discreet 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 FOR ALERTS ON OBJECTS

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

2.2.2. Checking for multiple alerts

While dealing with potential multiple alerts, care shall be taken to distinguish accurately between persons or objects that 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 following procedure shall apply:

(a) if processing a request for entering a new alert reveals that there is already a person or an object in the SIS II with the same identity description elements a more detailed check shall be run before the new alert is entered;

(b) in case of alerts on persons, if necessary, the SIRENE Bureau shall contact the SIRENE Bureau of the issuing Member State to clarify whether the alert relates to the same person (**E form**);

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

The following identity elements shall be compared when establishing the existence of multiple alerts on a person:

— surname,
— forename,
— date of birth,
— sex,
— national identity document number,
— forenames and surnames of parents,
— place of birth,
— fingerprints,
— photographs.

The following identity elements shall be compared when establishing the existence of multiple alerts on a vehicle:

— the VIN number,
— the registration number, and country of registration,
— the make,
— the type.

If, when entering a new alert, it is found that the same VIN number and/or registration plate number already exist in the SIS II, it shall be assumed that there are potential multiple alerts on the same vehicle. However, this method of verification is only effective where the description elements used are the same; therefore, the comparison is 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 automatically mean that there is a hit; and a negative response does not mean that there is not an alert on the vehicle.

For other objects, the most appropriate fields for identifying multiple alerts are the mandatory fields, all of which shall be used for automatic comparison by the system.

2.2.3. Entering multiple alerts

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 II in accordance with national procedure.

If the alerts are issued by different Member States, the following procedure shall apply:

(a) if the alerts are compatible, the SIRENE Bureaux do not need to consult one another;

(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 delete them when the new alert is entered. Any disputes shall be settled by Member States via SIRENE Bureaux. If agreement cannot be reached on the basis of the list of priorities established, the oldest alert shall be left in the SIS II;

(e) Member States who were not able to enter an alert may subscribe to be notified by the CS-SIS about the deletion of the alert;

(f) the SIRENE Bureau of the Member State that was not able to enter the alert may request that the SIRENE Bureau of the Member State that entered the alert informs it of a hit on this alert.

2.3. The exchange of information after a hit

A 'hit' occurs when an end-user conducts a search in the SIS II and finds out that an alert exists which matches the details entered and further action needs to be taken.

If the end-user requires supplementary information after a hit, the SIRENE Bureau shall contact the SIRENE Bureau of the issuing Member State as quickly as possible and ask for the necessary information. Where appropriate, the SIRENE Bureaux shall act as intermediaries between the national authorities and shall provide and exchange supplementary information pertinent to the alert in question.

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

The following procedure shall apply:

(a) without prejudice to Section 2.4 of this Manual, a hit on an individual or an object for which an alert has been issued, shall in principle be communicated to the SIRENE Bureau of the issuing Member State using a **G form**.

When notifying the issuing Member State of a hit, the applicable article of the SIS II legal instruments should be indicated in heading 090 of the **G form**.

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

If the hit concerns a person who is the subject of an alert for arrest, 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**;

(b) The SIRENE Bureaux of Member States that have issued alerts for refusal of entry shall not necessarily be informed of any hits as a matter of course, but may be informed in exceptional circumstances. A **G form** may in any case be sent if for example supplementary information is required. A **G Form** shall always be sent when there is a hit on a person benefiting from the Community right of free movement.

2.3.1. Communicating further information

The exchange of information under the SIS II legal instruments shall not prejudice the tasks entrusted to the SIRENE Bureaux by national law implementing other legal instruments of the European Union, in particular in application of the national law implementing Council

Framework Decision 2006/960/JHA[(2)] or, if this information falls within the scope of the mutual legal assistance.

2.4. When the procedures following a hit cannot be followed (Article 48 of the SIS II Decision and Article 33 of the SIS II Regulation)

In accordance with Article 48 of the SIS II Decision and Article 33 of the SIS II Regulation, the following procedure shall apply:

(a) the Member State that is unable to follow the procedure shall immediately inform the Member State that issued the alert via its SIRENE Bureau that it is not able to perform the requested action, and give the reasons by using an **H form**;

(b) the Member States concerned may then agree on the action to be taken in keeping with their own national legislation and with the provisions of the SIS II legal instruments.

2.5. Processing of data for purpose other than that for which it was entered in the SIS II (Article 46(5) of the SIS II Decision)

The data contained in the SIS II may only be processed for the purposes laid down for each category of alert.

However, if prior authorisation has been obtained from the issuing Member State, the data may be processed for a purpose other than that for which it was entered, in order to prevent an imminent serious threat to public policy and security, for serious reasons of national security or for the purposes of preventing a serious criminal offence.

If a Member State wants to process data in the SIS II for purpose other than that for which it was entered, the exchange of information shall take place according to the following rules:

(a) through its SIRENE Bureau, the Member State that wants to use data for a different purpose shall explain to the Member State that issued the alert the grounds for having the data processed for another purpose, by using an **I form**;

(b) as soon as possible, the issuing Member State shall study whether this wish can be met and inform the other Member State, through its SIRENE Bureau, of its decision;

(c) if need be, the Member State that issued the alert may 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 other Member State shall only use the data for the reason it sought and obtained authorisation. It shall take account of any conditions set by the issuing Member State.

2.6. Adding a flag (Articles 24 and 25 of the SIS II Decision)

At the request of another Member State add a flag.

Articles 24 and 25 of the SIS II Decision 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 for arrest (Article 26 of the Decision), alerts for missing persons (Article 32 of the Decision) and alerts for discreet or specific checks (Article 36 of the Decision) when it considers that giving effect to the alert would be incompatible with its national law, its international obligations or essential national interests. The reasons for the request shall be provided simultaneously.

An alternative procedure exists only for alerts for arrest. Each Member State shall detect the alerts likely to require a flag as swiftly as possible.

If the circumstances mentioned in Article 24(1) or 25 of the SIS II Decision no longer exist, the Member State that requested the flag shall ask as soon as possible for the flag to be revoked.

2.6.1. Consulting the Member States with a view of adding a flag

The following procedure shall apply:

(a) if a Member State requires a flag to be added, it shall request the flag from the issuing Member State using an **F form**, mentioning the reason for the flag;

(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, deleted or the request may be withdrawn.

2.6.2. Temporary clause until 1 January 2009: systematic request for flags to be added to alerts on a Member State's nationals

The following procedure has been adopted:

(a) a Member State may ask the SIRENE Bureau of the other Member State to add a flag as a matter of course to alerts for arrest issued on its nationals;

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

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

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

2.7. Data found to be legally or factually inaccurate (Article 34 of the SIS II Regulation and Article 49 of the SIS II Decision)

If data is found to be factually incorrect or has been unlawfully stored in the SIS II, then the exchange of supplementary information shall take place in line with the rules set out in Article 34(2) of the SIS II Regulation and 49(2) of the SIS II Decision, which provide that only the Member State that issued the alert may modify, add to, correct, update or delete data.

The Member State which found that data contains an error or that it has been unlawfully stored shall inform the issuing Member State via its SIRENE Bureau at the earliest opportunity and not later than 10 calendar days after the evidence suggesting the error has come to its attention. The exchange of information should be carried out using a **J form**.

(a) Following the result of consultations, the issuing Member State may have to delete or correct the data, in accordance with its national procedures for correcting the item in question;

(b) if there is no agreement within two months, the SIRENE Bureau of the Member State that discovered the error or that the data has been unlawfully stored shall advise the authority responsible within its own country to refer the matter to the European Data Protection Supervisor, who shall, jointly with the national supervisory authorities concerned, act as mediator.

Exchange of information following discovery of new facts

In order to ensure the data quality and the lawfulness of the data processing, if a new fact related to an alert comes to the attention of a SIRENE Bureau other than the SIRENE Bureau of the issuing Member State, it shall communicate this information as soon as possible to the SIRENE Bureau of the issuing Member State using a **J form**. This could happen, for example, when a third-country national on whom an alert for refusal of entry or stay has been issued, becomes a beneficiary of the Community right of free movement after the alert was issued.

2.8. The right to access and rectify data (Articles 41 of the SIS II Regulation and 58 of the SIS II Decision)[(3)]

The right of persons to have access to data, which relates to them and has been entered in the SIS II in accordance with the SIS II legal instruments, shall be exercised in accordance with the law of the Member State before which they invoke that right.

The individual concerned shall be informed as soon as possible and in any event within 60 calendar days from the date on which he/she applied for access, or sooner if national law so provides.

A Member State, which has not issued the alert, may communicate information to the person concerned only if it has previously given the Member State issuing the alert an opportunity to state its position.

Any person has the right to have factually inaccurate data relating to him or her corrected or to have unlawfully stored data relating to him or her deleted.

The individual shall be informed about the follow-up given to the exercise of these rights as soon as possible and in any event not later than three months from the date of his/her original application. The individual shall be informed sooner if national law so provides.

2.8.1. Requests for access to or rectification of data

Without prejudice to national law, if the national authorities are to be informed of a request to access or rectify data, then the exchange of information will take place according to the following rules:

(a) each SIRENE Bureau applies its national legislation on the right to access personal data. Depending on the circumstances of the case and in accordance with the applicable legislation, the SIRENE Bureaux shall either forward any requests they receive for access to or for rectification of data to the competent national authorities, 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, in accordance with their national law, forward them information on exercising the right to access data.

2.8.2. Exchange of information on requests for access to alerts issued by other Member States

As far as it is possible, information on requests for access to alerts entered into the SIS II by another Member State shall be exchanged via the national SIRENE Bureaux using a **K form**.

The following procedure shall apply:

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

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

(c) it shall take into account any deadlines for processing the request set by the Member State that received the request for access.

If the Member State that issued the alert sends its position to the SIRENE Bureau of the Member State that received the request for access, the SIRENE Bureau, according to national legislation and within the limits of its remit, shall either adjudicate upon the request or shall ensure that the position is forwarded to the authority responsible for adjudication of the request as soon as possible.

2.8.3. Exchange of information on requests to rectify or delete data entered by other Member States

When a person requests to have his or her data rectified or deleted, this may only be done by the Member State that issued the alert. If the person addresses a Member State other than the one that issued the alert, the SIRENE Bureau of the requested Member State shall inform the person about the need to contact the issuing Member State and shall provide him or her with the contact details of the competent authority of the issuing Member State.

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

Alerts entered into SIS II shall be kept only for the time required to meet the purposes for which they were supplied.

Excluding the cases after a hit, an alert shall be deleted either automatically by the CS-SIS (once the expiry date has passed) or directly by the service that entered the alert in the SIS II (once the conditions for the alert being maintained no longer apply).

In both instances the CS-SIS deletion message shall be processed automatically by the N.SIS II.

Member States have the possibility to subscribe to an automatic notification of the deletion of an alert issued by another Member State.

2.10. Entering proper names

Within the constraints imposed by national systems for entry of data, proper names (forenames and surnames) shall be entered into SIS II in a format (script and spelling) as close as possible to the format used on official identity documents. Member States shall use, as a general rule, Latin characters for entering data into SIS II, without prejudice to transliteration and transcription rules laid down in Annex 1.

2.11. Different categories of identity
Confirmed identity (established identity)

A confirmed identity (established identity) means that the identity has been confirmed on the basis of genuine ID documents, by passport or by statement from competent authorities.
Not confirmed identity

A not confirmed identity means that there is not sufficient proof of the identity.
Misused identity

A misused identity (surname, forename, date of birth) occurs if a person uses the identity of another real person. This can happen for example when a document is used to the detriment of the real owner.
Alias

Alias means an assumed identity used by a person known under other identities.

2.11.1. Misused identity (Article 36 of the SIS II Regulation and 51 of the SIS II Decision)

Subject to the person's consent, as soon as it is clear that a person's identity has been misused, additional data shall be added to the alert in the SIS II in order to avoid the negative consequences of misidentification. The person whose identity has been misused may, according to national procedures, provide the competent authority with the information specified in Article 36(3) of the SIS II Regulation and Article 51(3) of the SIS II Decision. Any person whose identity has been misused has the right to withdraw his/her consent for the information to be processed.

When a Member State discovers that an alert on a person issued by another Member State relates to a case of misused identity, it shall thereof inform the SIRENE Bureau of the issuing Member State using a **Q form**, in order that the data can be added to the SIS II alert.

The data of the person whose identity has been misused shall only be available for the purpose of establishing the identity of the person being checked and shall in no way be used for any other purpose. Information on misused identity shall be deleted at the same time as the alert or earlier if the person concerned so requests.

Taking into account the purpose for entering data of this nature, the photographs and fingerprints of the person whose identity has been misused should be added to the alert. On the **Q form**, only the Schengen number refers to the data of the person sought by the SIS II alert. The information in heading 052 (Date document was issued) is compulsory.

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

2.11.2. Entering an alias

To ensure sufficient data quality, Member States shall as far as possible inform each other about aliases and exchange all relevant information about the real identity of the sought subject.

The Member State that entered the alert shall be responsible for adding any aliases. If another Member State discovers an alias, it shall pass the matter on to the Member State that entered the alert.

In the case of alerts for arrest, the Member States adding the alias may inform all the other Member States about it by using an **M form**.

2.11.3. Further information to establish a person’s identity

The SIRENE Bureau of the issuing Member State may also, if the data in the SIS II is insufficient, provide further information after consultation, on its own initiative or at the request of another Member State, to help establish a person’s identity. The **L Form** shall be used for this purpose. This information shall, in particular, cover the following:

— the origin of the passport or identity document in the possession of the person sought,
— the passport or identity document’s reference number, issuing date, place and authority as well as the expiry date,
— description of the person sought,
— surname and forename of the wanted person's mother and father,
— last known address.

As far as possible, this information shall be available in the SIRENE Bureaux, or immediately and permanently accessible to them for speedy transmission.

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

2.12. Exchange of information in case of interlinked alerts

Article 37 of the SIS II Regulation and Article 52 of the SIS II Decision provide Member States with the possibility to create links between different alerts, in accordance with their national legislation, with a view to revealing relationships among persons and objects entered into the SIS II. Such links shall only be created when there is a clear operational need.

2.12.1. Technical rules

Each link allows for the establishment of a relationship between at least two alerts.

A Member State may create a link between alerts that it enters in the SIS II and only this Member State may modify and delete the link. Links shall only be visible to users when at least two alerts in the link are visible to them. Member States shall ensure that only authorised access to links is possible.

2.12.2. Operational rules

Links between alerts do not require special procedures for the exchange of supplementary information. Nevertheless the following principles shall be observed:

In case there is a hit on two or more interlinked alerts, the SIRENE Bureau of the executing Member State shall send a **G form** for each of them.

No forms shall be sent on alerts which, although linked to an alert on which there was a hit, were not respectively the object of the hit. This rule shall not apply in the case when a linked alert for which there was no hit is an alert for arrest or for a missing person (protection). In this case the communication of the discovery of the linked alert shall be carried out using an **M form**.

2.13. SIRPIT (SIRENE PIcture Transfer) and format and quality of biometric data in SIS II

Fingerprints and pictures shall be added to the alert entered into the SIS II when available.

SIRENE Bureaux shall be able to exchange fingerprints and pictures for the purpose of completing the alert. When a Member State has a picture or fingerprints of a person for whom an alert has been issued by another Member State, it may send the pictures and fingerprints via SIRPIT in order to allow the issuing Member State to complete the alert.

This exchange takes place without prejudice to the exchange in the framework of police cooperation in application of the Council Framework Decision 2006/960/JHA.

2.13.1. Further use of the data exchanged, including archiving

Any further use of pictures and fingerprints exchanged via SIRPIT, including archiving, shall comply with the relevant provisions of the SIS II legal instruments, Directive 95/46/EC, Convention 108 of the Council of Europe and with the legislation in force in that area in the Member States concerned.

2.13.2. Technical requirements

Fingerprints and pictures shall be collected and transmitted in accordance with the standards to be defined in the implementing rules for entering biometric data in the SIS II.

Every SIRENE Bureau should fulfil the SIRPIT technical requirements.

Fingerprints and pictures shall be sent in an attachment on an input screen, specially designed for SIRPIT.

2.13.3. Use of the SIRENE L form

The transmission 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.

2.13.4. SIRPIT procedure

The SIRENE Bureau of the country who has fingerprints or pictures of the person for whom an alert was issued by another Member State is known hereafter as 'the providing SIRENE Bureau'.

The SIRENE Bureau of the country, which has entered the alert into the SIS II, is known hereafter as 'SIRENE Bureau of the issuing Member State'.

The following procedure shall apply:

(a) the providing SIRENE Bureau shall send an **L form** through the usual electronic path and shall mention in field 083 of the **L form** that the fingerprints and pictures are being sent to complete the alert in the SIS II;

(b) the SIRENE Bureau of the issuing Member State shall add the fingerprints or pictures to the alert in the SIS II or shall send them to the competent authority to complete the alert.

2.13.4.1. Input screen

The input mask shall have the following data:

(1) Schengen ID number (*) ([1]);

(2) reference number (*) ([1]);

(3) date of fingerprints;

(4) place where fingerprints were taken;

(5) date of picture;

(6) reason for fingerprints;

(7) surname (*) ([2]);

(8) forename (*) ([2]);

(9) maiden name;

(10) identity ascertained?;

(11) date of birth (*);

(12) place of birth;

(13) nationality;

(14) gender (*);

(15) additional information;

Remarks:

(*) Mandatory

([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.

2.13.5. Format and quality of biometric data

All biometric data entered into the system shall have undergone a specific quality check to ensure a minimum quality standard common to all SIS II users.

Before entry, checks shall be carried out at the national level to ensure that:

— fingerprint data is compliant with the ANSI/NIST — ITL 1-2000 specified format, as implemented for the purposes of Interpol and adapted for SIRPIT (SIRENE Picture Transfer),

— photographs, that shall only be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS II, are compliant with the following requirements: full frontal face pictures aspect rate shall be, as far as possible, 3:4 or 4:5. When available, a resolution of at least 480 × 600 pixels with 24 bits of colour depth shall be used. If the image has to be acquired through a scanner, the image size shall be, as far as possible, less than about 200 Kbytes.

2.14. Overlapping roles of SIRENE and Interpol[(4)]

The role of the SIS II 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 the national level.

The following principles shall apply:

2.14.1. Priority of SIS II alerts over Interpol alerts

In case of alerts issued by Member States, SIS II 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.

2.14.2. Choice of communication channel

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

2.14.3. Use and distribution of Interpol diffusions in Schengen States

Given the priority of SIS II alerts over Interpol alerts, the use of 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 II, or where not all the necessary information is available to form a SIS II alert). Parallel alerts in the SIS II and via Interpol within the Schengen area should be avoided. Alerts which are distributed via Interpol channels and which also cover the Schengen area or parts thereof shall bear the following indication: '**except for the Schengen States**'.

2.14.4. Hit and deletion of an alert

In order to ensure the SIRENE Bureau's role as a coordinator of the verification of the quality of the information entered in the SIS II Member States shall ensure that the SIRENE Bureaux and the NCBs inform each other of hits and deletion of alerts.

2.14.5. Improvement of cooperation between the SIRENE Bureaux and the Interpol NCBs

In accordance with national law, each Member State shall take all appropriate measures to provide for the effective exchange of information at the national level between its SIRENE Bureau and the NCBs.

2.14.6. Sending information to third States

(a) Data processed in the SIS II.

According to Article 39 of the SIS II Regulation and 54 of the SIS II Decision, data processed in the SIS II in application of these two legal instruments shall not be transferred or made available to third countries or to international organisations. Article 55 of the SIS II Decision foresees derogation from this general rule regarding the exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol, subject to the conditions laid down in this article.

(b) Supplementary information

In accordance with the ‘data ownership principle’ contained in Article 4(2) of the SIS II legal instruments, transmission of supplementary information to third States shall be performed by the Member State ‘owner’ of the data. If a request for supplementary information related to a particular alert is received by the SIRENE Bureau of a State other than that issuing the alert, the former shall inform the latter of the request for information in order to allow the issuing Member State to take decision in full compliance with the applicable rules, including the rules on data protection. Use of the Interpol channel will depend on national provisions or procedures.

2.15. Relations of SIRENE and Europol

The Europol has the right to access and to directly search data entered into the SIS II according to SIS II Decision Articles 26, 36 and 38. Europol may request further information from the Member States concerned in accordance with the provisions of the Europol Convention. In accordance with national legislation, cooperation with the National Europol Unit (ENU) shall be established in order to ensure that the SIRENE Bureau is informed of any exchange of supplementary information between Europol and the ENU concerning alerts in the SIS II. In case communication on national level concerning SIS II alerts is done by the ENU, confusion of end-users shall be avoided.

2.16. Relations of SIRENE and Eurojust

The national members of Eurojust and their assistants have the right to access and to directly search data entered into the SIS II according to Decision Articles 26, 32, 34 and 38. In accordance with national law, cooperation with them shall be established in order to ensure a smooth exchange of information in case of a hit. In particular, the SIRENE Bureau shall be the contact point for national members of Eurojust and their assistants for supplementary information related to alerts in the SIS II.

2.17. Special types of search

2.17.1. Geographically targeted search

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

Geographically targeted searches in the Schengen area shall take place on the basis of an alert in the SIS II. If the whereabouts are known when issuing an alert for arrest, field 061 of the **A Form** shall include the information on whereabouts of the wanted person. In all other cases, including for communicating the whereabouts of objects, the **M form** (field 83) shall be used. An alert for the wanted person shall be entered in the SIS II to ensure that a request for action to be taken is immediately enforceable (Article 64 of the Schengen Convention, Article 9(3) of the Framework decision on EAW).

An alert in the SIS II increases the chances of success should the person or object move unexpectedly from one place to another within the Schengen area, so the non-entering of a wanted person or object into SIS II is possible only in special circumstances (e.g. in accordance with Article 23(1) of the SIS II Regulation and SIS II Decision if there is not enough information to create an alert, etc.).

(**1**) This text is identical to the text in the Annex to Commission Decision 2008/333/EC (see page 4 of this Official Journal).

(**2**) 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.

(**3**) Some information on access and rectifications procedures in the Member States can be found on the Commission's website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

(**4**) See also EU Schengen Catalogue, vol. 2: Schengen Information System, SIRENE: recommendations and best practices, December 2002.