ANNEX

SIRENE MANUAL

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)[(1)] 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[(2)]. 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[(3)]

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[(4)].

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)[(5)]. 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[(6)], C[(7)] and D[(8)] forms shall not be used any longer and are removed from Annex 5.

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

The SIRENE bureau shall answer all requests for information made by the other Member States via their SIRENE bureaux as soon as possible. In any event, a response shall be given within 12 hours. 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[9].
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[10].

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.

(**1**) See footnote 1.

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

(**3**) 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).

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

(**5**) 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).

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

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

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

(**9**) 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.

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