COMMISSION DECISION

of 4 March 2008

adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II)

(2008/334/JHA)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty on European Union,

Having regard to Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [1], and in particular Articles 8(4), 9(1), 20(4), 22(a), 38(3), 51(4) and 52(7) thereof,

Whereas:

(1) Decision 2007/533/JHA shall apply to Member States participating in SIS 1+ from dates to be fixed by the Council, acting by unanimity of its Members representing the Governments of the Member States participating in SIS 1+. These dates shall be fixed after, amongst other conditions to be met, the necessary implementing measures have been adopted by the Commission.

(2) These implementing measures cover SIS II aspects which, due to their technical nature, level of detail and need for regular updating, are not covered exhaustively by Decision 2007/533/JHA.

(3) These implementing measures include the SIRENE Manual which contains detailed rules for the exchange of supplementary information Supplementary information is information not stored in SIS II but connected to SIS II alerts, which is to be exchanged: in order to allow Member States to consult or inform each other when entering an alert; following a hit in order to allow the appropriate action to be taken; when the required action cannot be taken; when dealing with the quality of SIS II data; when dealing with the compatibility and priority of alerts; when dealing with rights of access.

(4) Other implementing measures are protocols and technical procedures ensuring the compatibility of N.SIS II with CS-SIS; technical rules necessary for entering, updating, deleting and searching data on persons and objects; the specification of the special quality check to ascertain the fulfilment of a minimum data-quality standard by photographs and fingerprints entered into the SIS II; technical rules on entering and further processing additional data for the purpose of dealing with misused identity and technical rules on the linking of alerts.

(5) The SIRENE Manual should be an important tool for SIRENE operators in their daily work with SIS II. It should have a form of a practical handbook and serve the purpose of facilitating the work of the SIRENE Bureau in its entirety.

(6) Since certain rules of a technical nature have a direct impact on the work of end-users in the Member States it is appropriate to combine them in one document.

(7) This Decision constitutes the necessary basis for adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) in respect of matters falling within the scope of the Treaty on European Union (EU Treaty). Commission Decision 2008/333/EC [2] adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) constitutes the necessary basis in respect of matters falling within the scope of the Treaty establishing the European Community (EC Treaty). The fact that the basis necessary for adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) consists of two separate instruments shall not affect the principle that these implementing measures constitute one single document. Nevertheless, for the sake of clarity the annex should be reproduced in the Annexes to both Decisions.

(8) The United Kingdom is taking part in this Decision, in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8 (2) of 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 provisions of the Schengen *acquis* [3].

(9) Ireland is taking part in this Decision in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 6(2) of Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* [4].

[1] OJ L 205, 7.8.2007, p. 63.

[2] See page 1 of this Official Journal.

[3] OJ L 131, 1.6.2000, p. 43.

[4] OJ L 64, 7.3.2002, p. 20.

(10) This Decision constitutes an act building on the Schengen *acquis* or otherwise related to it within the meaning of Article 3(2) of the 2003 Act of Accession and Article 4(2) of the 2005 Act of Accession.

(11) As regards Iceland and Norway, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* [1], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC [2] on certain arrangements for the application of that Agreement.

(12) As regards Switzerland, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point G of Decision 1999/437/EC of 25 October 2004 read in conjunction with Article 4(1) of the Council decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement [3].

(13) The measures provided for in this Decision are in accordance with the opinion of the Committee, set up by Article 67 of Council Decision 2007/533/JHA.

HAS DECIDED AS FOLLOWS:

Sole article

For the purposes of matters falling within the scope of the EU Treaty, the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) shall be as set out in the Annex.

Done at Brussels, 4 March 2008.

For the Commission
Franco FRATTINI
Vice-President

[1] OJ L 176, 10.7.1999, p. 36.
[2] OJ L 176, 10.7.1999, p. 31.
[3] OJ L 368, 15.12.2004, p. 26.

ANNEX

SIRENE Manual and other implementing measures [1]

TABLE OF CONTENTS

INTRODUCTION 44

The Schengen *acquis* 44

The second generation Schengen Information System (SIS II) 45

Supplementary information 46

1. **THE SIRENE BUREAUX AND THE SIS II** 47

1.1. The SIRENE Bureau 47

1.2. SIRENE Manual 47

1.3. Other implementing measures 47

1.4. Standards 47

1.4.1. Availability 47

1.4.2. Continuity 47

1.4.3. Security 48

1.4.4. Confidentiality 48

1.4.5. Accessibility 48

1.4.6. Communications 48

1.4.7. Transliteration rules 49

1.4.8. Data quality 49

1.4.9. Structures 49

1.4.10. Archiving 49

1.5. Staff 50

1.5.1. Knowledge 50

1.5.2. Recruitment 50

1.5.3. Training 50

1.5.4. Exchange of staff 50

1.6. Technical infrastructure 50

1.6.1. Data exchange between SIRENE Bureaux 51

1.7. Training of other services 51

2. **GENERAL PROCEDURES** 51

2.1. Definitions 51

2.2. Multiple Alerts (Article 34(6) of the SIS II Regulation and 49(6) of the SIS II Decision) 51

2.2.1. Compatibility of alerts and order of priority 51

2.2.2. Checking for multiple alerts 53

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

2.2.3. Entering multiple alerts . . . 54

2.3. The exchange of information after a hit . . . 55

2.3.1. Communicating further information . . . 55

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) . . . 55

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) . . . 56

2.6. Adding a flag (Articles 24 and 25 of the SIS II Decision) . . . 56

2.6.1. Consulting the Member States with a view of adding a flag . . . 56

2.6.2. Temporary clause until 1 January 2009: systematic request for flags to be added to alerts on a Member State's nationals . . . 57

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) . . . 57

Exchange of information following discovery of new facts . . . 57

2.8. The right to access and rectify data (Articles 41 of the SIS II Regulation and 58 of the SIS II Decision) 57

2.8.1. Requests for access to or rectification of data . . . 58

2.8.2. Exchange of information on requests for access to alerts issued by other Member States . . . 58

2.8.3. Exchange of information on requests to rectify or delete data entered by other Member States . . . 58

2.9. Deleting when the conditions for maintaining the alert cease to be met . . . 58

2.10. Entering proper names . . . 58

2.11. Different categories of identity . . . 59

2.11.1. Misused identity (Article 36 of the SIS II Regulation and 51 of the SIS II Decision) . . . 59

2.11.2. Entering an alias . . . 59

2.11.3. Further information to establish a person's identity . . . 59

2.12. Exchange of information in case of interlinked alerts . . . 60

2.12.1. Technical rules . . . 60

2.12.2. Operational rules . . . 60

2.13. SIRPIT (SIRENE PIcture Transfer) and format and quality of biometric data in SIS II . . . 60

2.13.1. Further use of the data exchanged, including archiving . . . 60

2.13.2. Technical requirements . . . 61

2.13.3. Use of the SIRENE **L form** . . . 61

2.13.4. SIRPIT procedure . . . 61

2.13.5. Format and quality of biometric data . . . 62

2.14. Overlapping roles of SIRENE and Interpol . . . 62

2.14.1. Priority of SIS II alerts over Interpol alerts . . . 62

2.14.2. Choice of communication channel . . . 62

2.14.3. Use and distribution of Interpol diffusions in Schengen States . . . 62

2.14.4. Hit and deletion of an Alert . . . 62

2.14.5. Improvement of cooperation between the SIRENE Bureaux and the Interpol NCBs . . . 62

2.14.6. Sending information to Third States . . . 63

2.15. Relations of SIRENE and Europol . . . 63

2.16. Relations of SIRENE and Eurojust . . . 63

2.17. Special types of search . . . 63

2.17.1. Geographically targeted search . . . 63

3. **ALERTS FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES (ARTICLE 26 OF THE SIS II DECISION)** . . . 63

3.1. Entering an alert . . . 64

3.2. Multiple alerts . . . 64

Compatibility of alerts for arrest . . . 64

3.3. Misused identity . . . 65

3.4. Entering an alias . . . 65

3.5. Supplementary information to be sent to Member States . . . 65

3.5.1. Supplementary information to be sent with regards to an EAW . . . 65

3.5.2. Supplementary information to be sent with regards to provisional arrest . . . 66

3.6. Adding a flag . . . 66

3.7. Action by SIRENE Bureaux upon receipt of an alert for arrest . . . 66

3.8. The exchange of information after a hit . . . 66

4. **ALERTS FOR REFUSAL OF ENTRY OR STAY (ARTICLE 24 OF THE SIS II REGULATION)** 67

4.1. Entering an alert . . . 67

4.2. Multiple alerts . . . 67

Compatibility of alerts for refusal of entry or stay . . . 67

4.3. Misused identity . . . 67

4.4. Entering an alias . . . 67

4.5. Exchange of information following a hit . . . 68

4.5.1. Exchange of information when issuing residence permits or visas . . . 68

4.5.2. Exchange of information when refusing entry or expelling from the Schengen territory . . . 69

4.6. Exchange of information following a hit on a third-country national who is a beneficiary of the Community right of free movement . . . 70

4.7. Deletion of alerts entered for EU citizens . . . 70

5. **ALERTS ON MISSING PERSONS (ARTICLE 32 OF THE SIS II DECISION)** . . . 70

5.1. Entering an alert . . . 71

5.2. Multiple alerts . . . 71

Compatibility of alerts on missing persons . . . 71

5.3. Misused identity . . . 71

5.4. Entering an alias . . . 71

5.5. Adding a flag . . . 71

5.6. The exchange of information after a hit . . . 71

6. **ALERTS FOR PERSONS SOUGHT FOR A JUDCIAL PROCEDURE (ARTICLE 34 OF THE SIS II DECISION)** ... 72

6.1. Entering an alert ... 72

6.2. Multiple alerts ... 72

Compatibility of alerts for a judicial procedure ... 72

6.3. Misused identity ... 72

6.4. Entering an alias ... 73

6.5. The exchange of information after a hit ... 73

7. **ALERTS FOR DISCREET AND SPECIFIC CHECKS (ARTICLE 36 OF THE SIS II DECISION)** 73

7.1. Entering an alert ... 73

7.2. Multiple alerts ... 73

Compatibility of alerts for checks ... 74

7.3. Misused identity ... 74

7.4. Entering an alias ... 74

7.5. Informing other Member States when issuing alerts requested by authorities responsible for national security (Article 36(3) of the Decision) ... 74

7.6. Adding a flag ... 74

7.7. The exchange of information after a hit ... 74

8. **ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE (ARTICLE 38 OF THE SIS II DECISION)** ... 74

8.1. Entering an alert ... 75

8.2. Multiple alerts ... 75

Compatibility of alerts for seizure and use as evidence ... 75

8.3. The exchange of information after a hit ... 75

9. **STATISTICS** ... 75

10. **REVISION OF THE SIRENE MANUAL AND OTHER IMPLEMENTING MEASURES** ... 75

INTRODUCTION

The Schengen *acquis*

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.

[1] OJ L 239, 22.9.2000, p. 19.

Subsequently, as of 26 March 1995, the Schengen *acquis* was fully applied in Belgium, Germany, France, Luxembourg, Netherlands, Spain and Portugal [1]. As of 31 of March 1998, in Austria and Italy [2]; as of 26 of March 2000 in Greece [3] and finally, as of 25 March 2001, the Schengen *acquis* was applicable in full in Norway, Iceland, Sweden, Denmark and Finland [4].

The United Kingdom (UK) and Ireland only take part in some of the provisions of the Schengen *acquis*, in accordance with Decision 2000/365/EC and Decision 2002/192/EC respectively.

In the case of the UK, the provisions in which the United Kingdom wished to take part (with exception of SIS) are applicable as of the 1 January 2005 [5].

The Schengen *acquis* was incorporated into the legal framework of the European Union by means of protocols attached to the Treaty of Amsterdam [6] 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), and 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.

Some of the provisions of the Schengen *acquis* apply upon accession of new States to the EU. Other provisions shall only apply in these Member States pursuant to a Council decision to that effect. Finally, the Council takes a decision on the lifting of border checks, after verification that the necessary conditions for the application of all parts of the *acquis* concerned have been met in the Member State in question, in accordance with the applicable Schengen evaluation procedures and after consultation of the European Parliament.

In 2004, the Swiss Confederation signed an agreement with the European Union and the European Community concerning its association with the implementation, application and development of the Schengen *acquis* [7], which shall be read in conjunction with Decision 2004/860/EC.

The second generation Schengen Information System (SIS II)

The SIS II, set up pursuant to the provisions of Regulation (EC) No 1987/2006 of the European Parliament and of the Council [8] and Council Decision 2007/533/JHA [9] (hereinafter jointly referred to as the SIS II legal instruments) constitutes a common information system allowing the competent authorities in the Member States to cooperate by exchanging information, and, is an essential tool for the application of the provisions of the Schengen *acquis* as integrated into the framework of the European Union. It replaces the first generation Schengen Information System that began operating in 1995 and was extended in 2005 and 2007.

Its purpose as laid down in Article 1 of the aforementioned legal Acts is '(…) to ensure a high level of security within an area of freedom, security and justice of the European Union including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the (EC) Treaty (hereinafter referred to as EC Treaty) relating to the movement of persons in their territories, using information communicated via this system'.

---

(1) 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).

(2) 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.

(3) 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).

(4) 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).

(5) 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).

(6) OJ C 340, 10.11.1997.

(7) OJ L 370, 17.12.2004, p. 78.

(8) Hereinafter called 'SIS II Regulation'.

(9) OJ L 205, 7.8.2007, p. 63. Hereinafter called 'SIS II Decision'.

In accordance with the aforementioned SIS II legal instruments, by means of an automated consultation procedure, the SIS II shall provide access to alerts on persons and objects to the following authorities:

(a) authorities responsible for border controls, in accordance with Regulation (EC) No 562/2006 of the European Parliament and the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders [1];

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

(c) national judicial authorities and their coordination authorities;

(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 Community *acquis* relating to the movement of persons;

(e) authorities responsible for issuing vehicle registration certificates (in accordance with the Regulation (EC) No 1986/2006 of the European Parliament and of the Council [2]).

In accordance with the SIS II Decision, Europol and Eurojust also have access to certain categories of alerts. Both Europol and Eurojust may access data entered into SIS II in accordance with Articles 26 (alerts for arrest) and 38 (alerts for seizure or use as evidence). In addition, Europol may also access data entered in accordance with Article 36 (alerts for discreet or specific checks); and Eurojust may access data entered in accordance with Article 32 (alerts on missing persons) and Article 34 (alerts for a judicial procedure).

The SIS II is made up of the following components:

1. a central system (the Central SIS II) composed of:

2. a technical support function (CS-SIS) containing a database, the 'SIS II database';

3. a uniform national interface (NI-SIS);

4. a national system (N.SIS II) in each of the Member States, consisting of the national data systems which communicate with the Central SIS II. An N.SIS II may contain a data file (a national copy), containing a complete or partial copy of the SIS II database;

5. a communication infrastructure between the CS-SIS and the NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux as defined below.

Supplementary information

The SIS II only contains the indispensable information (i.e. alert data) allowing the identification of a person or an object and the necessary action to be taken. In addition, according to the SIS II legal instruments, Member States shall exchange supplementary information related to the alert which is required for implementing certain provisions foreseen under the SIS II legal instruments, and for the SIS II to function properly, either on a bilateral or multilateral basis.

This structure built to deal with the exchange of supplementary information has been given the name 'SIRENE', which is an acronym of the definition of the structure in English: Supplementary Information REquest at the National Entries.

According to the SIS II legal instruments the supplementary information shall be exchanged in the following cases:

(a) in order to allow Member States to consult or inform each other whilst entering an alert (e.g. when entering alerts for arrest);

(b) following a hit in order to allow the appropriate action to be taken (e.g. matching an alert);

(c) when the required action cannot be taken (e.g. adding a flag);

(d) when dealing with the quality of SIS II data (e.g. when data has been unlawfully entered or is factually inaccurate);

[1] OJ L 105, 13.4.2006, p. 1.
[2] OJ L 381, 28.12.2006, p. 1.

(e) when dealing with the compatibility and priority of alerts (e.g. when checking for multiple alerts);

(f) when dealing with the exercise of the right of access.

1. THE SIRENE BUREAUX AND THE SIS II

1.1. The SIRENE Bureau

A national 'SIRENE Bureau' shall be set up by each of the Member States in accordance with Article 7(2) of the SIS II legal instruments. It shall serve as a single contact point for the Member States for the purpose of exchanging supplementary information. Its main tasks are [1]:

1. to ensure the exchange of all supplementary information in accordance with the provisions of this SIRENE Manual, as provided in Article 8 of the SIS II legal instruments;

2. to coordinate the verification of the quality of the information entered into the SIS II.

The SIS II operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system (CS-SIS).

However, it is necessary for the Schengen Member States to be able to exchange, either on a bilateral or multilateral basis, supplementary information required for implementing certain provisions laid down in the SIS II legal instruments in order for the SIS II to function properly.

1.2. SIRENE Manual

The SIRENE Manual is a set of instructions for the SIRENE Bureaux, which describes in detail the rules and procedures governing the bilateral or multilateral exchange of supplementary information. It constitutes an implementing measure necessary for the operational use of the SIS II as laid down in the SIS II legal instruments.

Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 51(2) of SIS II Regulation and Article 67 of SIS II Decision and in the form of a manual called the 'SIRENE Manual'.

1.3. Other implementing measures

Certain aspects of SIS II such as technical rules on entering data, including data required for entering an alert, updating, deleting and searching data, rules on compatibility and priority of alerts, the adding of flags, links between alerts and the exchange of supplementary information cannot be covered exhaustively by the SIS II Regulation and SIS II Decision, owing to their technical nature, level of detail and need for regular updating. Implementing powers in respect of those aspects should therefore be delegated to the Commission.

Since certain rules of a technical nature have a direct impact on the work of end-users in the Member States, it is appropriate to include such rules in the SIRENE Manual. Therefore Annexes 1, 2, and 4 to this Manual shall set out rules on transliteration, code tables, and other technical implementing measures for data processing, respectively.

1.4. Standards

The fundamental standards that underpin the cooperation via SIRENE shall be as follows:

1.4.1. *Availability*

A national SIRENE Bureau shall be fully operational 24 hours a day, seven days a week. Provision of technical analysis, support and solutions shall also be available 24 hours a day, seven days a week.

1.4.2. *Continuity*

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

[1] This is without prejudice to other tasks given to SIRENE Bureaux based on respective legislation in the framework of police cooperation, e.g. in the application of the Council Framework Decision 2006/960/JHA (OJ L 386, 29.12.2006, p. 89).

The heads of SIRENE Bureaux shall meet at least twice a year to assess the quality of the cooperation between their services, to discuss necessary technical or organisational measures in the event of any difficulties and to clarify procedures where required.

1.4.3. *Security*

According to Article 10(2) of the SIS II legal instruments, with respect to the exchange of supplementary information, Member States are obliged to take security measures equivalent to those to be taken in relation to their N.SIS II as provided for in Article 10(1).

Recommendations and best practices laid down in Volume 2 of the 'EU Schengen Catalogue: Schengen Information System, SIRENE' should be as far as possible reflected in practice.

The SIRENE Bureau system should have a back-up computer and database system at a secondary site in case of a serious emergency at the SIRENE Bureau.

Physical and organisational security features are necessary to protect the SIRENE Bureau premises. In order to meet the security requirements, as provided for in the SIS II legal instruments, appropriate requirements regarding security on the premises shall apply. The specific features of these requirements may differ as they will have to adapt against threats in the immediate surroundings and according to the exact location of the SIRENE Bureau. They may therefore include the following; however, this list is not exhaustive:

— external windows fitted with security glass,

— secured and closed doors,

— brick/concrete walls enclosing the SIRENE Bureau,

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

— security guards on site or rapidly available,

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

— dedicated premises to avoid persons who are not involved in international police cooperation measures, or who do not have requisite access from having to enter or to pass through the SIRENE Bureau offices,

— sufficient back-up power supply.

The specific measures to be adopted in the application of article 10(2) of the SIS II legal instruments shall be determined by each Member State. Member States shall monitor the effectiveness of these security measures and take the necessary organisational measures related to internal monitoring, to ensure compliance with the SIS II legal instruments.

1.4.4. *Confidentiality*

Pursuant to Article 11 of the SIS II legal instruments, relevant national rules of professional secrecy or other equivalent obligations of confidentiality shall apply to all SIRENE personnel. This obligation shall also apply after those people leave office or employment.

1.4.5. *Accessibility*

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

1.4.6. *Communications*

Pursuant to Article 4(1)(c) of the SIS II legal instruments SIRENE Bureaux shall use an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux for their communication. Only if this channel is not available, another adequately secured, and given the circumstances, the most appropriate means of communication may be used. The ability to choose the channel means that it shall be determined on a case by case basis, according to technical possibilities and the security and quality requirements that the communications have to meet.

Written messages shall be divided into two categories: free text and standard forms. The latter shall be set out as in Annex 3.

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

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

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

In addition, the SIRENE Bureau shall use a dedicated and secure e-mail for the exchange of all information not exchanged via forms.

1.4.7. *Transliteration rules*

The transliteration rules set out in Annex 1 shall be respected.

1.4.8. *Data quality*

Pursuant to Article 7(2) of the SIS II legal instruments, SIRENE Bureaux shall coordinate the verification of the quality of the information entered in the SIS II. SIRENE Bureaux shall have the necessary national competence to perform this role. Therefore, an adequate form of national data quality audit shall be provided for, including a review of the rate of alerts/hits and of data content.

In order to allow each SIRENE Bureau to perform its role of data quality verification co-ordinator, the necessary IT support and appropriate rights within the systems should be available.

1.4.9. *Structures*

All national authorities, including SIRENE Bureaux, responsible for international police cooperation should be organised in a structured way so as to prevent conflicts of powers with other national bodies carrying out similar functions and to prevent the duplication of work.

1.4.10. *Archiving*

(a) Each Member State shall establish conditions for storing information;

(b) the SIRENE Bureau of the Member State issuing the alert shall keep all of the information on its own alerts available to the other Member States, including a reference to the decision giving rise to the alert;

(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) 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. As a rule, this information shall be deleted immediately after the related alert has been deleted from the SIS II, and in any event at the latest one year thereafter. 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 other Member States shall be stored according to national data protection legislation in the recipient Member State. The relevant provisions of the SIS II legal instruments, the Directive 95/46/EC of the European Parliament and of the Council [1] and the Convention 108 of the Council of Europe [2] shall also apply.

(f) Access to archives shall be controlled and restricted to designated staff.

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

[2] Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and subsequent amendments thereto.

1.5. **Staff**

1.5.1. *Knowledge*

SIRENE Bureau staff shall have 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, European and international legal aspects,

— their national law enforcement authorities, and

— national and European judiciary and immigration administration systems.

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

Operators on duty outside office hours shall have the same competence, knowledge and authority and it should be possible for them to refer to experts available on-call.

Legal expertise to cover both normal and exceptional cases should be available in the SIRENE Bureau. Depending on the case, this may be provided by any personnel with the necessary legal background or experts from judicial authorities.

1.5.2. *Recruitment*

The responsible national recruiting authorities have to take all the above skills and knowledge into consideration when recruiting new staff and, consequently, organise in-service training courses or sessions at both national and European level.

A high level of experienced staff leads to a workforce able to function on their own initiative and thereby able to handle cases efficiently. Therefore a low turnover of personnel is desired, which requires the unambiguous support of management to create a devolved working environment.

1.5.3. *Training*

National level

At the national level, sufficient training shall ensure that staff meets the required standards laid down in this Manual. Before being authorised to process data stored in the SIS II, staff shall in particular receive appropriate training about data security and data protection rules and shall be informed of any relevant criminal offences and penalties.

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, share information on national working methods and create a consistent and equivalent level of knowledge. It will furthermore make staff aware of the importance of their work and the need for mutual solidarity in view of the common security of Member States.

1.5.4. *Exchange of staff*

As far as possible, SIRENE Bureaux shall also foresee setting up staff exchanges with other SIRENE Bureaux at least once a year. These exchanges are intended to help improve staff knowledge of working methods, to show how other SIRENE Bureaux are organised and to establish personal contacts with colleagues in other Member States.

1.6. **Technical infrastructure**

Each SIRENE Bureau shall have a computerised management system, which allows a great deal of automation in the management of the daily workflow.

1.6.1. *Data exchange between SIRENE Bureaux*

The technical specifications concerning the exchange of information between SIRENE Bureaux are laid down in the 'Data exchange between SIRENE Bureaux' ([1]).

1.7. **Training of other services**

SIRENE Bureaux should be involved in establishing national standards for the training of end-users on data quality principles and practices as well as in the training of all authorities entering alerts, stressing data quality, data protection requirements and the maximum utilisation of the SIS II.

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.

([1]) Doc. 16375/07.

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 [1] 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.

[1] 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.

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)** [1]

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.

[1] 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.

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** [1]

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.

[1] See also EU Schengen Catalogue, vol. 2: Schengen Information System, SIRENE: recommendations and best practices, December 2002.

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.).

3. **ALERTS FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES (ARTICLE 26 OF THE SIS II DECISION)**

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

— misused identity,

— entering an alias,

— supplementary information to be sent to Member States,

— adding a flag,

— action by SIRENE Bureau upon receipt of an alert for arrest,

— the exchange of information after a hit.

3.1. **Entering an alert**

Most of the alerts for arrest will be accompanied by a European Arrest Warrant (EAW). However, under an alert for arrest, a provisional arrest is also possible prior to obtaining an Extradition Request (ER).

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

When entering an alert for arrest for surrender purposes, a copy of the original EAW shall be entered as an attachment into the SIS II. A translated copy of the EAW in one or more of the official languages of the institutions of the EU may be entered.

In addition, photographs and fingerprints of the person shall be added to the alert when available.

The relevant information including EAW or ER, provided with regard to persons wanted for arrest for surrender or extradition purposes, shall be available to the SIRENE Bureau when the alert is entered. A check shall be made to ensure that the information is complete and correctly presented.

Member States shall be able to enter more than one EAW per alert for arrest. It is the responsibility of the Member States to delete an EAW that loses its validity and to check if there are any other European Arrest Warrants attached to the alert and extend the alert if needed.

Alerts for arrest may contain one binary file per EAW. Member States shall be able to attach translations of any European Arrest Warrants they attach to an alert for arrest and if necessary in separate binary files.

For scanned PDF documents that are to be attached to alerts, as far as possible, a minimum resolution of 150 DPI shall be used.

3.2. **Multiple alerts**

For general procedures see Section 2.2.

In addition, the following rules shall apply:

several Member States may enter an alert for arrest on the same person. If two or more Member States have issued an alert 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.

Compatibility of alerts for arrest

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

Alerts for arrest shall be entered immediately without awaiting the result of any consultation with other Member States.

3.3. **Misused identity**

See general procedure in Section 2.11.1.

3.4. **Entering an alias**

See general procedure in Section 2.11.2.

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

When issuing the alert, supplementary information regarding the alert shall be sent to all Member States.

The information mentioned in Sections 3.5.1 and 3.5.2 shall be sent to the other SIRENE Bureaux by the swiftest means available. Any further information required for identification purposes shall be sent after consultation and/or at the request of another Member State.

In the case where several EAWs or ERs exist for the same person, separate A forms shall be completed for each of the EAWs or ERs.

There shall be sufficient detail contained in the EAW/ER 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', field 044: 'description of the deeds') for other SIRENE Bureaux to verify the alert. However, only the necessary information shall be exchanged.

3.5.1. *Supplementary Information to be sent with regards to an EAW*

The **A form** shall contain at least the same information as that in the EAW. The information in field 044 shall contain a short summary of the circumstances.

In an **A form**:

— 239: it shall be indicated that the form relates only to an EAW,

— 272: a sequence number of the EAW shall be entered in order to distinguish between several EAWs for the same person,

— 006-013, 266, 275, 237-238 and 050-061: the relevant information inserted in the SIS II and corresponding to Section (a) of the EAW shall be entered,

— 030-033 and 251-259: the relevant information from Section (i) of the EAW shall be entered,

— 240-241 and 035-037: the relevant information from Section (b) of the EAW shall be entered,

— 034, 038, 039: the relevant information from Section (c) of the EAW shall be entered,

— 243-244: information from Section (d) of the EAW shall be entered. If there was no decision in absentia, the fields shall be left empty. In field 244 a simple description can be entered without copying the text of the law,

— 245, 247, 040-045 and 047: information from Section (e) of the EAW shall be entered,

— 267: information from Section (f) shall be entered. The text of the relevant legal provisions shall not be copied,

— 249: the relevant information from Section (g) shall be entered. If there is no request for seizure of property, the field shall be left empty,

— 250: the relevant information from Section (g) shall be entered. If known, also the location of the property shall be mentioned,

— 268: the relevant information from Section (h) shall be entered,

— 260-264: the relevant information from Section (i) shall be entered,

— 269-271: the relevant information from Section (i) shall be entered but only in case it is different from fields 251, 252 and 032),

— 400 and 403: additional documents may be attached.

3.5.2. *Supplementary information to be sent with regards to provisional arrest*

3.5.2.1. When issuing an alert based on both an EAW and an ER

When issuing the alert for arrest for extradition purposes, supplementary information shall be sent to all Member States using an **A form**. If the data in the alert and the supplementary information sent to Member States with regard to an EAW is not sufficient for extradition purposes, additional information shall be provided.

In field 239 it shall be indicated that the form relates to both an EAW and an ER.

3.5.2.2. When issuing an alert based on ER only

When issuing the alert for arrest for extradition purposes, supplementary information shall be sent to all Member States using an **A form**.

In field 239 it shall be indicated that the form relates to an ER.

3.6. **Adding a flag**

For general rules see Section 2.6.

If at least one of the EAWs or ERs attached to the alert can be executed, the alert shall not be flagged.

A flagged alert shall be regarded as being issued for the purposes of communicating the whereabouts of the person for whom it was issued.

3.7. **Action by SIRENE Bureaux upon receipt of an alert for arrest**

When a SIRENE Bureau receives an **A form**, it shall, as soon as possible, search all available sources to try and locate the subject. If the information provided by the issuing Member State is not sufficient for acceptance by the receiving Member State, this shall not prevent the searches being carried out.

If the alert for arrest is validated and the subject is located or arrested in the Member State, then the information contained in the **A form** should be forwarded to the competent authority of the Member State which executes the EAW or the ER. If the original EAW or ER is requested, it should be sent by the issuing judicial authority directly to the executing judicial authority (unless otherwise provided for in the national law of the issuing or executing Member State).

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

See general procedure in Section 2.3.

In addition, the following procedure shall apply:

(a) a 'hit' on an individual for whom an alert for arrest has been issued should always be communicated immediately to the SIRENE Bureau of the issuing Member State. Moreover, after sending the **G form**, it should also communicate the hit to the SIRENE Bureau of the issuing Member State by telephone;

(b) if necessary the SIRENE Bureau of the issuing Member State shall then send any relevant, specific information on the particular measures that shall be taken by the SIRENE Bureau of the executing Member State.

In addition, the SIRENE Bureau of the issuing Member State shall inform all other SIRENE Bureaux of the hit, using an **M form**, provided that the hit occurred within two weeks of the date that the alert was issued. After this period, the information shall only be sent to these Member States that requested it.

4. ALERTS FOR REFUSAL OF ENTRY OR STAY (ARTICLE 24 OF THE SIS II REGULATION)

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

— misused identity,

— entering an alias,

— the exchange of information after a hit,

— special case of family member of EU citizens.

4.1. Entering an alert

In accordance with Article 24 of the SIS II Regulation, alerts for refusal of entry or stay may be entered in the SIS II for third-country nationals based on a national alert issued for reasons of a threat to public policy, public security or national security.

An alert may be also entered based on the fact that the third-country national has been subject to a measure involving expulsion, refusal of entry or removal which has not been rescinded or suspended, that includes or is accompanied by a prohibition on entry or residence, based on the failure to comply with national regulations on the entry or residence of third-country nationals.

In addition, Article 26 of the SIS II Regulation provides that, subject to certain specific conditions, alerts relating to third-country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the Treaty on European Union, shall also be entered.

According to Article 25 of the SIS II Regulation, specific rules apply to third-country nationals who are beneficiaries of the Community 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 [1]. The SIRENE Bureau shall as far as possible be able to make available any information that was used to assess whether an alert for refusal of entry or stay be entered for a beneficiary of the Community right of free movement [2].

4.2. Multiple alerts

See general procedure in Section 2.2.

Compatibility of alerts for refusal of entry or stay

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.

4.3. Misused identity

See general procedure in Section 2.11.1.

4.4. Entering an alias

For general rules see Section 2.11.2.

---

[1] OJ L 158, 30.4.2004, p. 77.

[2] Article 30 of the Directive 2004/38/EC provides that the person refused entry shall be notified in writing thereof and informed in full on grounds on which the decision was taken unless it is contrary to the interests of State security.

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

Carrying out the information procedures laid down under Article 5(4)(c) of the Schengen Border 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 for 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.

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

The following procedure shall apply:

(a) without prejudice to the special procedure concerning the exchange of information, which takes place in accordance with Article 25 of the Schengen Convention; and without prejudice to point 4.6, which concerns the exchange of information following a hit on a third-country national who is the beneficiary of the Community right of free movement (in which case the consultation of the SIRENE of the issuing Member State is obligatory); 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 visa. The Member State that issued the alert may then inform other Member States using an **M form** if appropriate;

(b) 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.

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

Procedure under article 25(1) of the Schengen Convention

If a Member State that is considering granting a residence permit 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.

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, it shall instigate a consultation procedure with the Member State that issued the residence permit, 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 discovers later that there is an alert for refusal of entry or stay on that person entered into the SIS II [1].

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

[1] 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 II 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 three 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 II data). Such enquiries shall not be made as a matter of routine.

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.

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

The following procedure shall apply:

(a) without prejudice to the special procedures concerning the exchange of information, which takes place in accordance with Article 5(4)(a) and (c) of the Schengen Borders Code; and without prejudice to point 4.6 which concerns the exchange of information following a hit on a third-country national who is the beneficiary of the Community right of free movement (in which case the consultation of the issuing Member State via its SIRENE Bureau is obligatory), 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 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 (see Section 2.8.3).

Special procedures as provided for in Article 5(4)(a) and (c) of the Schengen Borders Code

Procedure in cases falling under Article 5(4)(a)

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** 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 or re-entry visa, when crossing 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 II, 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 II 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 deletion of the alert.

If third-country national concerned tries to enter a third Member State, which is neither the State that issued the alert nor that one which granted the residence permit, and the third Member State finds out that there is an alert in the SIS II on that person albeit he/she has a residence permit issued by one of the Member States, it shall allow transit towards the Member State that issued the residence permit. 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 II or to withdraw the residence permit. It may also request to be informed of the result of any consultation.

Procedure in cases falling under Article 5(4)(c)

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 thereof the SIRENE Bureau of the issuing Member State using an **H form**.

4.6. Exchange of information following a hit on a third-country national who is a beneficiary of the Community right of free movement

If there is a hit on a third-country national who is beneficiary of the Community right of free movement within the meaning of Directive 2004/38/EC [1]:

(a) at the request of the competent authority, the SIRENE of the executing Member State shall immediately contact the SIRENE 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 of the issuing Member State shall immediately start gathering the required information and send it as soon as possible to the SIRENE of the executing Member State,

(c) the executing Member State shall inform via its SIRENE Bureau the SIRENE Bureau of the issuing Member State whether the requested action to be taken was carried out (using **G form**) or not (using **H form**).

4.7. 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 EU Member States, 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 2.7).

5. ALERTS ON MISSING PERSONS (ARTICLE 32 OF THE SIS II DECISION)

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

[1] According to Directive 2004/38/EC, a person benefiting from the Community 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. 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.

— misused identity,

— entering an alias,

— adding a flag,

— the exchange of information after a hit.

5.1. **Entering an alert**

At the request of the competent authority, data of the following categories of persons, both minors and adults, shall be entered in the SIS II for the purpose of ascertaining their whereabouts or placing them under protection:

— missing persons who need to be placed under protection:

(i) for their own protection;

(ii) in order to prevent threats,

— missing persons whose whereabouts need to be ascertained and who do not need to be placed under protection.

National procedures concerning who and how one can request a search for a missing person shall be followed accordingly, whilst the search is being initiated.

In accordance with Article 23(2) of the SIS II Decision, photographs and fingerprints of the person shall be added to the alert when available.

5.2. **Multiple alerts**

See general procedure in Section 2.2.

Compatibility of alerts on missing persons

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 or alerts for checks.

5.3. **Misused identity**

See general procedure in Section 2.11.1.

5.4. **Entering an alias**

See general procedure in Section 2.11.2.

5.5. **Adding a flag**

A flag may be requested after a hit has occurred. With a view to adding a flag, the general procedures as described in Section 2.6 shall be followed.

There is no alternative action to be taken for alerts for missing persons.

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

See general procedure in Section 2.3.

In addition the following rules shall apply:

(a) as far as it is possible, the SIRENE Bureaux shall communicate the necessary medical details of the missing person(s) concerned if measures have to be taken for their protection.

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

(b) the SIRENE Bureau of the executing Member State shall always communicate the whereabouts to the SIRENE Bureau of the issuing Member State;

(c) in accordance with Article 33(2) of the SIS II Decision, the communications of the whereabouts of the missing person who is of age to the person who reported the person missing shall be subject to the missing person's consent. However, the competent authorities may communicate the fact that the alert has been deleted following a hit, to the person who reported him or her missing.

6. ALERTS FOR PERSONS SOUGHT FOR A JUDCIAL PROCEDURE (ARTICLE 34 OF THE SIS II DECISION)

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

— misused identity,

— entering an alias,

— the exchange of information after a hit.

6.1. Entering an alert

At the request of the competent authority, data of the following categories of persons shall be entered into the SIS II for the purpose of communicating their place of residence or domicile:

— witnesses,

— persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted,

— persons who are to be served with a criminal judgement or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted,

— persons who are to be served with a summons to report in order to serve a penalty involving deprivation of liberty.

In accordance with Article 23(2) of the SIS II Decision, photographs and fingerprints of the person shall be added to the alert when available.

6.2. Multiple alerts

See general procedure in Section 2.2.

Compatibility of alerts for a judicial procedure

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.

6.3. Misused identity

See general procedure in Section 2.11.1.

6.4. **Entering an alias**

See general procedure in Section 2.11.2.

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

See general procedure in Section 2.3.

In addition, the following rules shall apply:

(a) the real 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) as opposed to alerts on missing persons, no consent is required for communication of the place of residence or domicile to the competent authorities.

7. ALERTS FOR DISCREET AND SPECIFIC CHECKS (ARTICLE 36 OF THE SIS II DECISION)

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

— misused identity,

— entering an alias,

— information exchange when issuing alerts at the request of authorities responsible for State security,

— adding a flag;

— the exchange of information after a hit.

7.1. **Entering an alert**

At the request of the competent authority, data on persons and objects (vehicles, boats, aircrafts and containers) may be entered in the SIS II for the purpose of discreet checks and specific checks.

A specific check is a thorough check of the persons, vehicles, boats, and aircrafts, whereas a discreet check shall be carried out without jeopardising its discreet nature.

Such alerts may be entered for the purpose of prosecuting criminal offences and for the prevention of threats to public security in cases specified in Article 36(2) of the SIS II Decision.

Alerts for discreet and specific checks may also be issued at the request of the authorities responsible for national security in accordance with Article 36(3) of the SIS II Decision.

In accordance with Article 37(4) of the SIS II Decision, if execution of specific checks is not authorised under the law of a Member State, they shall automatically be replaced, in that Member State, by discreet checks.

In accordance with Article 23(2) of the SIS II Decision, photographs and fingerprints of the person shall be added to the alert when available.

7.2. **Multiple alerts**

See general procedure in Section 2.2.

Compatibility of alerts for checks

Alerts on persons for discreet 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.

Alerts on objects for discreet or specific checks are not compatible with other categories of alerts.

Alerts for discreet checks are not compatible with alerts for specific checks.

7.3. **Misused identity**

See general procedure in Section 2.11.1.

7.4. **Entering an alias**

See general procedure in Section 2.11.2.

7.5. **Informing other Member States when issuing alerts requested by authorities responsible for national security (Article 36(3) of the Decision)**

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**. The form shall contain the name of the authority requesting entry of the alert and its contact details.

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

7.6. **Adding a flag**

See general procedure in Section 2.6.

There is no alternative action to be taken for alerts for discreet or specific checks.

In addition, if the State security service in the executing Member State decides that the alert requires a validity flag, they shall contact their national SIRENE Bureau and inform it that the required action to be taken cannot be carried out. The SIRENE Bureau shall then request a flag by sending an **F form** to the SIRENE Bureau of the issuing Member State. It shall not be necessary to explain the reasons for the flag.

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

See general procedure in Section 2.3.

In addition the following rules shall apply:

when a hit occurs on an alert issued pursuant to Article 36(3) of the SIS II Decision, the SIRENE Bureau of the executing Member State shall inform the SIRENE Bureau of the issuing Member State of the results (for either discreet or specific check) via the **G form**. At the same time the SIRENE Bureau of the executing Member State shall inform its own competent service responsible for national security.

8. **ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE (ARTICLE 38 OF THE SIS II DECISION)**

The following steps shall be considered:

— entering an alert,

— check for multiple alerts,

— the exchange of information after a hit.

8.1. **Entering an alert**

Data on the following objects may be entered into the SIS II for the purpose of seizure or use as evidence in criminal proceedings:

— motor vehicles with a cylinder capacity exceeding 50 cm^3, boats and aircrafts,

— trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers,

— firearms;

— blank official documents, which have been stolen misappropriated or lost,

— issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents, which have been stolen, misappropriated, lost or invalidated,

— vehicle registration certificates and vehicle number plates, which have been stolen, misappropriated, lost or invalidated,

— banknotes (registered notes),

— securities and means of payment such as cheques, credit cards, bonds, stocks and shares, which have been stolen, misappropriated, lost or invalidated.

8.2. **Multiple alerts**

See general procedure in Section 2.2.

Compatibility of alerts for seizure and use as evidence

Alerts for seizure or use as evidence are incompatible with alerts for checks.

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

If requested, the SIRENE Bureaux shall send supplementary information as quickly as possible via a **P form**, in response to a **G form** when a hit is made on an alert for seizure or use as evidence issued on a vehicle, aircraft, boat or container pursuant to Article 36 of the SIS II Decision.

Given that the request is urgent and that it will not therefore be possible to collate all the information immediately, it shall not be necessary to fill all the fields of the **P form**. However, efforts shall be made to collate the information relating to the main headings: 041, 042, 043, 162, 164, 165, 166, 167 and 169.

9. **STATISTICS**

Once a year the SIRENE Bureaux shall provide statistics, which have to be sent to the Management Authority and the Commission. The statistics shall also be sent, upon request, to the European Data Protection Supervisor and the competent National Data Protection Authorities.

The statistics shall comprise the number of forms of each type sent to each of the Member States. In particular, the statistics shall show the number of hits and flags. A distinction shall be made between hits found on alerts issued by another Member State and hits found by a Member State on alerts it issued.

10. **REVISION OF THE SIRENE MANUAL AND OTHER IMPLEMENTING MEASURES**

The Manual and other implementing measures shall be revised if it becomes necessary to modify some of the provisions in order to ensure smooth operations.