

This document is meant purely as a documentation tool and the institutions do not assume any liability for its contents

► **B**

**COMMISSION IMPLEMENTING DECISION**

**of 26 February 2013**

**on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II)**

*(notified under document C(2013) 1043)*

**(Only the Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish texts are authentic)**

**(2013/115/EU)**

**(OJ L 71, 14.3.2013, p. 1)**

Amended by:

					Official Journal			
					No	page	date	
► <b><u>M1</u></b>	Commission January 2015	Implementing	Decision	2015/219/EU of 29	L 44	75	18.2.2015	



# COMMISSION IMPLEMENTING DECISION

of 26 February 2013

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

*(notified under document C(2013) 1043)*

**(Only the Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish texts are authentic)**

(2013/115/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)<sup>(1)</sup>, and in particular Articles 8(4), 9(1) and 20(3), point (a) of Article 22 and Articles 36(4) and 37(7) thereof, and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)<sup>(2)</sup>, and in particular Articles 8(4), 9(1) and 20(4), point (a) of Article 22 and Articles 51(4) and 52(7) thereof,

Having consulted the European Data Protection Supervisor,

Whereas:

- (1) The second generation Schengen Information System (SIS II) will enter into operation in the first half of 2013. It will only contain the indispensable information allowing the identification of a person or an object and the necessary action to be taken. In addition, for SIS II to function properly, Member States will exchange supplementary information related to the alerts. This exchange of supplementary information is carried out by the Sirene Bureaux.
- (2) To facilitate the work of the Sirene Bureaux and of users of SIS II involved in Sirene operations in their daily work, a Sirene Manual for SIS II was adopted in 2008 through a former first pillar legal instrument, Commission Decision 2008/333/EC<sup>(3)</sup>, as well as a former third pillar instrument, Commission Decision 2008/334/JHA<sup>(4)</sup>.

<sup>(1)</sup> OJ L 381, 28.12.2006, p. 4.

<sup>(2)</sup> OJ L 205, 7.8.2007, p. 63.

<sup>(3)</sup> OJ L 123, 8.5.2008, p. 1.

<sup>(4)</sup> OJ L 123, 8.5.2008, p. 39.

**▼B**

- (3) Amendments to the Sirene Manual for SIS II are required now in order to better reflect the operational needs of users and staff involved in Sirene operations, to improve consistency of working procedures and to ensure that technical rules correspond to the state of the art.
  
- (4) Member States have developed diverging rules about authorities having access to SIS II empowered to create, update or delete alerts. Furthermore, many Member States have integrated offices for international police cooperation including Europol, Interpol and Sirene matters in which staff carry out all necessary operations. It is therefore appropriate to extend the scope of the Sirene Manual to all users of SIS II and to all staff involved in Sirene operations.
  
- (5) The provisions of the Sirene Manual need to be revised in order to reflect, inter alia, new technical capabilities for carrying out searches in SIS II; an updated description of the technical means of communication between Sirene Bureaux; clarification on procedures for alerts for refusal of entry; clarified procedures on management of SIS II alerts including the new categories of object introduced by Regulation (EC) No 1987/2006 and Decision 2007/533/JHA; procedures for exchanging supplementary information when it becomes clear that a SIS II alert concerns a vehicle that has been subject of criminal replication of vehicle details.
  
- (6) To ensure the compliance of transcription and transliteration rules between SIS II and Sirene the rules on transcription and transliteration should be fully aligned with ICD 3.0 for SIS II, the latest version of the Interface Control Document referred to in Council Regulation (EC) No 189/2008 of 18 February 2008 on the tests of the second generation Schengen Information System (SIS II) <sup>(1)</sup>. Furthermore, the forms to be used by Sirene Bureaux for their exchanges of supplementary information should be aligned with the technical architecture set out in the document: 'Data exchange between Sirene Bureaux (DEBS)'. These forms should also use a more comprehensible, user-friendly format. It is moreover appropriate to set out an explanation of the procedures for gathering statistics on SIS II hits and on the exchange of supplementary information and to attach these explanations to the Manual as a new appendix.
  
- (7) Due to the number of substantial changes made to the Sirene Manual for SIS II adopted in 2008 it is appropriate to adopt a new Sirene Manual. Therefore, Decisions 2008/333/EC and 2008/334/JHA should be repealed.

<sup>(1)</sup> OJ L 57, 1.3.2008, p. 1.

## ▼B

- (8) Provisions on the protection of personal data and security of data in SIS II are set out in Regulation (EC) No 1987/2006 and Decision 2007/533/JHA. In the absence of specific provisions in Regulation (EC) No 1987/2006, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>(1)</sup> should apply to the exchange of supplementary information in relation to alerts based upon Article 24 of Regulation (EC) No 1987/2006. In the absence of specific provisions in Decision 2007/533/JHA, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters<sup>(2)</sup> should apply to the exchange of supplementary information relating to all other alerts.
- (9) Given that Regulation (EC) No 1987/2006 builds upon the Schengen *acquis*, Denmark, in accordance with Article 5 of the Protocol on the position of Denmark annexed to the Treaty on European Union and the Treaty establishing the European Community, notified by letter of 15 June 2007 the transposition of this *acquis* into its national law. Denmark participates in Decision 2007/533/JHA. It is therefore bound to implement this Decision.
- (10) The United Kingdom is taking part in this Decision to the extent that it does not concern the exchange of supplementary information in relation to Articles 24 and 25 of Regulation (EC) No 1987/2006, in accordance with Article 5 of the Protocol on the Schengen *acquis* integrated into the framework of the European Union annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, 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*<sup>(3)</sup>.
- (11) Ireland is taking part in this Decision to the extent that it does not concern the exchange of supplementary information in relation to Articles 24 and 25 of Regulation (EC) No 1987/2006, in accordance with Article 5 of the Protocol on the Schengen *acquis* integrated into the framework of the European Union annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, 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*<sup>(4)</sup>.
- (12) As regards Cyprus, this Decision constitutes an act building upon the Schengen *acquis* or otherwise related to it within the meaning of Article 3(2) of the 2003 Act of Accession.

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31.

<sup>(2)</sup> OJ L 350, 30.12.2008, p. 60.

<sup>(3)</sup> OJ L 131, 1.6.2000, p. 43.

<sup>(4)</sup> OJ L 64, 7.3.2002, p. 20.

## ▼B

- (13) 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 latter's association with the implementation, application and development of the Schengen *acquis* <sup>(1)</sup>, which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC <sup>(2)</sup> on certain arrangements for the application of that Agreement.
- (14) As regards Switzerland, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(3)</sup>, which falls within the area referred to in Article 1, point G of Decision 1999/437/EC read in conjunction with Article 4(1) of Council Decision 2004/860/EC <sup>(4)</sup>.
- (15) As regards Liechtenstein, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(5)</sup>, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU <sup>(6)</sup>.
- (16) The measures provided for in this Decision are in accordance with the opinion of the Committee set up by Article 51 of Regulation (EC) No 1987/2006 and Article 67 of Decision 2007/533/JHA,

HAS ADOPTED THIS DECISION:

*Article 1*

The Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II) shall be as set out in the Annex and the Appendices thereof. They shall be applicable to staff involved in Sirene operations as well as to all users of SIS II.

*Article 2*

Decisions 2008/333/EC and 2008/334/JHA are repealed.

<sup>(1)</sup> OJ L 176, 10.7.1999, p. 36.

<sup>(2)</sup> OJ L 176, 10.7.1999, p. 31.

<sup>(3)</sup> OJ L 53, 27.2.2008, p. 52.

<sup>(4)</sup> OJ L 370, 17.12.2004, p. 78.

<sup>(5)</sup> OJ L 160, 18.6.2011, p. 21.

<sup>(6)</sup> OJ L 160, 18.6.2011, p. 19.

*Article 3*

This Decision shall take effect on the day of its notification.

It shall apply from the date to be fixed by the Council, acting by unanimity of its Members representing the governments of the Member States participating in SIS 1 + in accordance with Article 55(2) of Regulation (EC) No 1987/2006 and Article 71(2) of Decision 2007/533/JHA.

*Article 4*

This Decision is addressed to the Kingdom of Belgium, the Republic of Bulgaria, the Czech Republic, the Kingdom of Denmark, the Federal Republic of Germany, the Republic of Estonia, Ireland, the Hellenic Republic, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Grand Duchy of Luxembourg, Hungary, the Republic of Malta, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Slovenia, the Slovak Republic, the Republic of Finland, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland.



## ANNEX

**The Sirene Manual and other implementing measures for the second  
generation Schengen Information System (SIS II)**

## TABLE OF CONTENTS

## INTRODUCTION

1. THE SIRENE BUREAUX AND SUPPLEMENTARY INFORMATION
  - 1.1. The Sirene Bureau
  - 1.2. Sirene Manual
  - 1.3. Appendices to this Sirene Manual
  - 1.4. Catalogue of recommendations for the correct application of the Schengen *acquis* and best practices (Schengen Information System)
  - 1.5. Role of the Sirene Bureaux in police cooperation in the European Union
    - 1.5.1. Transfer of SIS II data and supplementary information to third countries or international organisations
  - 1.6. Relations between Sirene Bureaux and Europol
  - 1.7. Relations between Sirene Bureaux and Eurojust
  - 1.8. Relations between Sirene Bureaux and Interpol
    - 1.8.1. Priority of SIS II alerts over Interpol alerts
    - 1.8.2. Choice of communication channel
    - 1.8.3. Use and distribution of Interpol diffusions in Schengen States
    - 1.8.4. Hit and deletion of an alert
    - 1.8.5. Improvement of cooperation between the Sirene Bureaux and the Interpol NCBs
  - 1.9. Standards
    - 1.9.1. Availability
    - 1.9.2. Continuity
    - 1.9.3. Confidentiality
    - 1.9.4. Accessibility
  - 1.10. Communications
    - 1.10.1. Language of communication
    - 1.10.2. Data exchange between Sirene Bureaux
    - 1.10.3. Network, messages and mailboxes
    - 1.10.4. Communication in exceptional circumstances
  - 1.11. Sirene Address Book (SAB)
  - 1.12. Sirene workflow system
  - 1.13. Time limits for response
    - 1.13.1. Indication of urgency in Sirene forms including urgent reporting of a hit
  - 1.14. Transliteration/transcription rules
  - 1.15. Data quality
  - 1.16. Archiving
  - 1.17. Staff
    - 1.17.1. Heads of Sirene Bureaux
    - 1.17.2. Sirene Contact Person (SIRCoP)

**▼ M1**

- 1.17.3. Knowledge
- 1.17.4. Training
- 1.17.5. Exchange of staff
- 2. GENERAL PROCEDURES
- 2.1. Definitions
- 2.2. Multiple Alerts (Article 34(6) of the SIS II Regulation and Article 49(6) of the SIS II Decision)
  - 2.2.1. Compatibility of alerts
  - 2.2.2. Order of priority of alerts
  - 2.2.3. Checking for incompatibility and entering multiple alerts
  - 2.2.4. Special situation of the United Kingdom and Ireland
- 2.3. The exchange of information after a hit
- 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)
- 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)
- 2.6. Flagging
  - 2.6.1. Introduction
  - 2.6.2. Consulting the Member States with a view to adding a flag
  - 2.6.3. A request for deletion of a flag
- 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)
- 2.8. The right to access and rectify data (Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision)
  - 2.8.1. Requests for access to or rectification of data
  - 2.8.2. Exchange of information on requests for access to alerts issued by other Member States
  - 2.8.3. Exchange of information on requests to rectify or delete data entered by other Member States
- 2.9. Deleting when the conditions for maintaining the alert cease to be met
- 2.10. Entering proper names
- 2.11. Different categories of identity
  - 2.11.1. Misused identity (Article 36 of the SIS II Regulation and Article 51 of the SIS II Decision)
  - 2.11.2. Entering an alias
  - 2.11.3. Further information to establish a person's identity
- 2.12. Exchange of information in case of interlinked alerts
  - 2.12.1. Operational rules
- 2.13. Format and quality of biometric data in SIS II



▼ **M1**

- 2.13.1. Further use of the data exchanged, including archiving
- 2.13.2. Exchanging fingerprints and photographs
- 2.13.3. Technical requirements
- 2.13.4. Format and quality of biometric data
- 2.14. Special types of search
  - 2.14.1. Geographically targeted search
  - 2.14.2. Search with participation of special police units for targeted search (FAST)
- 3. ALERTS FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES (ARTICLE 26 OF THE SIS II DECISION)
  - 3.1. Entering an alert
  - 3.2. Multiple alerts
  - 3.3. Misused identity
  - 3.4. Entering an alias
  - 3.5. Supplementary information to be sent to Member States
    - 3.5.1. Supplementary information to be sent with regard to provisional arrest
  - 3.6. Adding a flag
    - 3.6.1. Systematic request for a flag to be added to alerts on persons wanted for arrest for extradition purposes where Framework Decision 2002/584/JHA does not apply
  - 3.7. Action by Sirene Bureaux upon receipt of an alert for arrest
  - 3.8. The exchange of information after a hit
  - 3.9. Supplementary information exchange about surrender or extradition
  - 3.10. Supplementary information exchange about transit through another Member State
  - 3.11. Deletion of alerts upon surrender or extradition
- 4. ALERTS FOR REFUSAL OF ENTRY OR STAY (ARTICLE 24 OF THE SIS II REGULATION)
  - 4.1. Entering an alert
  - 4.2. Multiple alerts
  - 4.3. Misused identity
  - 4.4. Entering an alias
  - 4.5. Exchange of information when issuing residence permits or visas
    - 4.5.1. Procedure in cases falling under Article 5(4)(a)
    - 4.5.2. Procedure in cases falling under Article 5(4)(c)

**▼ M1**

- 4.6. Common rules concerning procedures referred to in Section 4.5
- 4.7. Exchange of information following a hit and when refusing entry or expelling from the Schengen area
- 4.8. Exchange of information following a hit on a third-country national who is a beneficiary of the right of free movement
- 4.9. Exchange of information if, in the absence of a hit, a Member State discovers that there is an alert for refusal of entry for a third-country national who is a beneficiary of the right of free movement
- 4.10. Deletion alerts for refusal of entry or stay
- 5. ALERTS ON MISSING PERSONS (ARTICLE 32 OF THE SIS II DECISION)
  - 5.1. Multiple alerts
  - 5.2. Misused identity
  - 5.3. Entering an alias
  - 5.4. Adding a flag
  - 5.5. Provision of descriptive detail on missing minors and other persons assessed as being at risk
  - 5.6. The exchange of information after a hit
  - 5.7. Deletion of alerts on missing persons
    - 5.7.1. Minors
    - 5.7.2. Adults where no protective measures are requested
    - 5.7.3. Adults, protective measures requested
- 6. ALERTS FOR PERSONS SOUGHT FOR A JUDICIAL PROCEDURE (ARTICLE 34 OF THE SIS II DECISION)
  - 6.1. Multiple alerts
  - 6.2. Misused identity
  - 6.3. Entering an alias
  - 6.4. The exchange of information after a hit
  - 6.5. Deletion of alerts on persons sought for a judicial procedure
- 7. ALERTS FOR DISCREET AND SPECIFIC CHECKS (ARTICLE 36 OF THE SIS II DECISION)
  - 7.1. Multiple alerts
  - 7.2. Misused identity
  - 7.3. Entering an alias
  - 7.4. Informing other Member States when issuing alerts
  - 7.5. Adding a flag
  - 7.6. The exchange of information after a hit
  - 7.7. Deletion of alerts on discreet and specific checks
  - 7.8. Automatic Number Plate Recognition systems (ANPR)

**▼ M1**

8. ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE (ARTICLE 38 OF THE SIS II DECISION)
  - 8.1. Multiple alerts
  - 8.2. Vehicle alerts
    - 8.2.1. Checking for multiple alerts on a vehicle
    - 8.2.2. VIN-twins
  - 8.3. The exchange of information after a hit
  - 8.4. Deletion of alerts on objects for seizure or use as evidence in criminal proceedings
9. AUTOMATIC NUMBER PLATE RECOGNITION SYSTEMS (ANPR)
10. STATISTICS

▼ **M1**

## INTRODUCTION

**The Schengen area**

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 <sup>(1)</sup> 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.

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

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 <sup>(6)</sup>.

The Schengen *acquis* was incorporated into the legal framework of the European Union by means of protocols attached to the Treaty of Amsterdam <sup>(7)</sup> 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 Latvia, the Republic of Lithuania, Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic. These Member States became full members of the Schengen area on 21 December 2007.

Cyprus is a signatory to the Convention implementing the Schengen Agreement but enjoys a derogation under its Act of Accession of 2003.

<sup>(1)</sup> OJ L 239, 22.9.2000, p. 19.

<sup>(2)</sup> Decision of the Executive Committee of 22 December 1994 on bringing into force the Convention implementing the Schengen Agreement of 19 June 1990 (SCH/Com-ex (94)29 rev. 2. (OJ L 239, 22.9.2000, p. 130).

<sup>(3)</sup> 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.

<sup>(4)</sup> 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).

<sup>(5)</sup> 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).

<sup>(6)</sup> Council Decision 2004/926/EC of 22 December 2004 on the 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).

<sup>(7)</sup> OJ C 340, 10.11.1997.

▼ **M1**

The Republic of Bulgaria and Romania acceded to the European Union on 1 January 2007; as from that date the Schengen *acquis* and the acts building upon it or otherwise related to it are binding upon them, with the derogation provided by their Act of Accession of 2005.

Croatia acceded to the European Union on 1 July 2013. It applies the Schengen *acquis* with the derogation provided by its Act of Accession of 2011.

Some of the provisions of the Schengen *acquis* apply upon accession of new Member 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.

Certain other European countries joined the Schengen area. The Kingdom of Norway and the Republic of Iceland concluded an Association Agreement with the Member States on 18 May 1999 <sup>(1)</sup> in order to be associated to the Schengen Convention.

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* <sup>(2)</sup>, based upon which it became a member of the Schengen area on 12 December 2008.

On the basis of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(3)</sup>, signed in 2008, the Principality of Liechtenstein became a member of the Schengen area on 19 December 2011.

### **The second generation Schengen Information System (SIS II)**

SIS II, set up pursuant to the Regulation (EC) No 1987/2006 and Decision 2007/533/JHA (SIS II Decision) on the establishment, operation and use of the Second Generation Information System (SIS II) (together: the SIS II legal instruments) as well as Regulation (EC) No 1986/2006 of the European Parliament and of the Council <sup>(4)</sup> constitute 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. These instruments as of 9 April 2013 when in application, repealed Title IV of the Convention implementing the Schengen Agreement. SIS II replaces the first generation Schengen Information System that began operating in 1995 and was extended in 2005 and 2007.

<sup>(1)</sup> Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 36).

<sup>(2)</sup> OJ L 370, 17.12.2004, p. 78.

<sup>(3)</sup> OJ L 160, 18.6.2011, p. 3.

<sup>(4)</sup> Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

▼ **M1**

The purpose of SIS II as laid down in Article 1 of the SIS II legal instruments 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 the EC Treaty) relating to the movement of persons in their territories, using information communicated via this system’.

In accordance with the SIS II legal instruments, by means of an automated consultation procedure, 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 of the Council <sup>(1)</sup>;
- (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 Union law relating to the movement of persons;
- (e) authorities responsible for issuing vehicle registration certificates (in accordance with Regulation (EC) No 1986/2006).

In accordance with the SIS II Decision, Europol and Eurojust also have access to certain categories of alerts.

SIS II is made up of the following components:

1. a central system (the Central SIS II) composed of:
  - (a) a technical support function (CS-SIS) containing a database (the SIS II database);
  - (b) a uniform national interface (NI-SIS);
2. 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;
3. a communication infrastructure between the CS-SIS and the NI-SIS that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between Sirene Bureaux as defined below.

<sup>(1)</sup> 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 (Schengen Borders Code) (OJ L 105, 13.4.2006, p. 1).

▼ **M1**

## 1. THE SIRENE BUREAUX AND SUPPLEMENTARY INFORMATION

1.1. **The Sirene Bureau**

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 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.

A national 'Sirene Bureau' shall be set up by each of the Member States in accordance with common Article 7(2) of the SIS II legal instruments. It shall serve as a single contact point for the Member States, fully operational on 24/7 basis, for the purpose of exchanging supplementary information in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons and objects have been entered in SIS II and are found as a result of a hit. The Sirene Bureaux's main tasks include<sup>(1)</sup> ensuring the exchange of all supplementary information is in accordance with the requirements of this Sirene Manual, as provided in common Article 8 of the SIS II legal instruments for the following purposes:

- (a) 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 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), including the validation of outgoing alerts and the verification of incoming alerts, if it is provided for by national law;
- (e) when dealing with the compatibility and priority of alerts (e.g. when checking for multiple alerts);
- (f) when dealing with data subjects' rights, in particular the right of access to data.

Member States are encouraged to organise all national bodies responsible for international police cooperation, including Sirene Bureaux, in a structured way so as to prevent conflicts of competence and duplication of work.

<sup>(1)</sup> 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 of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).

▼ **M1****1.2. Sirene Manual**

The Sirene Manual is a set of instructions which describes in detail the rules and procedures governing the bilateral or multilateral exchange of supplementary information.

**1.3. Appendices to this Sirene Manual**

Since certain rules of a technical nature have a direct impact on the work of users in the Member States, including the Sirene Bureaux, it is appropriate to include such rules in the Sirene Manual. Therefore Appendices to this Manual set out, inter alia, rules on transliteration, code tables, forms for communication of supplementary information and other technical implementing measures for data processing.

**1.4. Catalogue of recommendations for the correct application of the Schengen *acquis* and best practices (Schengen Information System)**

The catalogue serves to provide legally non-binding recommendations and best practices for Member States in the light of experience. It also serves as a reference tool for evaluation of the correct implementation of the SIS II legal instruments. Accordingly, it should, as far as possible, be followed.

**1.5. Role of the Sirene Bureaux in police cooperation in the European Union**

The exchange of supplementary information shall not prejudice the tasks entrusted to the Sirene Bureaux in the area of international police cooperation by national law implementing other legal instruments of the European Union.

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

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

**1.5.1. *Transfer of SIS II data and supplementary information to third countries or international organisations***

According to Article 39 of the SIS II Regulation and Article 54 of the SIS II Decision, data processed in SIS II in application of these two legal instruments shall not be transferred or made available to third countries or to international organisations. This prohibition shall apply to the transfer of supplementary information to third countries or 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.



▼ **M1****1.6. Relations between Sirene Bureaux and Europol**

Europol has the right to access and to directly search data entered in SIS II according to Articles 26, 36 and 38 of the SIS II Decision. Europol may request further information from the Member States concerned in accordance with the provisions of the Europol Decision<sup>(1)</sup>. In accordance with national law, it is strongly recommended that cooperation with the National Europol Unit (ENU) should 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 SIS II. In exceptional cases where communication at national level concerning SIS II alerts is done by the ENU, all parties to the communication, especially the Sirene Bureau, should be made aware of this fact to avoid confusion.

**1.7. Relations between Sirene Bureaux and Eurojust**

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

**1.8. Relations between Sirene Bureaux and Interpol<sup>(2)</sup>**

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:

**1.8.1. *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.

**1.8.2. *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.

<sup>(1)</sup> Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

<sup>(2)</sup> See also Schengen Catalogue, recommendations and best practices.

▼ **M1**1.8.3. *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 SIS II legal instruments 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'.

1.8.4. *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.

1.8.5. *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.

1.9. **Standards**

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

1.9.1. *Availability*

Each Sirene Bureau shall be fully operational 24 hours a day, seven days a week in order to be able to react within the time limit as required in Section 1.13. Provision of technical and legal analysis, support and solutions shall also be available 24 hours a day, seven days a week.

1.9.2. *Continuity*

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

1.9.3. *Confidentiality*

Pursuant to common 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 staff. This obligation shall also apply after staff members leave office or employment.

1.9.4. *Accessibility*

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

1.10. **Communications**1.10.1. *Language of communication*

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

▼ **M1**1.10.2. *Data exchange between Sirene Bureaux*

The technical specifications concerning the exchange of information between Sirene Bureaux are laid down in the document: 'Data exchange between Sirene Bureaux (DEBS)'. These instructions shall be respected.

1.10.3. *Network, messages and mailboxes*

Sirene Bureaux shall use an encrypted virtual network exclusively dedicated to SIS II data and the exchange of supplementary information between Sirene Bureaux, as referred to in common Articles 4(1)(c) and 8(1) of the SIS II legal instruments. Only if this channel is not available, another adequately secured and 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. Appendix 3 describes the forms exchanged between Sirene Bureaux and set out guidance on the expected content of the fields, including whether they are mandatory or not.

There shall be four different mailboxes within the abovementioned network for free text messages and Sirene forms.

Mailbox	Mailbox Address	Purpose
Operational	oper@xx.sirenemail2.eu	Used for the exchange of forms and attachments between Sirene Bureaux
Technical	tech@xx.sirenemail2.eu	Used for e-mail exchange between the technical support staff of the Sirene Bureaux
Head of Sirene	director@xx.sirenemail2.eu	Used for e-mail exchange with the Heads of the Sirene Bureaux
E-mail	message@xx.siren-email2.eu	Used for free text message exchange between Sirene Bureaux

For testing purposes a second domain exists <sup>(1)</sup> (testxx.sirenemail2.eu) within which any of the mailboxes in the table above may be replicated for test purposes without interfering with the live message exchange and workflow environment.

The detailed rules on Sirene mailboxes and transmission of Sirene forms described in DEBS shall apply.

<sup>(1)</sup> This second domain exists in the technical 'pre-production environment'.

▼ **M1**

The Sirene workflow system (see Section 1.12) shall monitor the operational and e-mail mailboxes ('oper' and 'message') to detect incoming forms, related e-mails and attachments. Urgent messages shall only be sent to the operational mailbox.

1.10.4. *Communication in exceptional circumstances*

Where normal communication channels are not available and it is necessary to send standard forms by fax, for example, the procedure described in DEBS shall apply.

1.11. **Sirene Address Book (SAB)**

The contact details of the Sirene Bureaux and relevant information for mutual communication and cooperation are collected and provided in the Sirene Address Book (SAB). The Commission will update the SAB. The updated SAB shall be issued by the Commission at least twice per year. Each Sirene Bureau shall ensure that:

- (a) information from the SAB is not disclosed to third parties;
- (b) the SAB is known and used by the Sirene staff;
- (c) any update of the information listed in the SAB is provided without delay to the Commission.

1.12. **Sirene workflow system**

The effective management of the Sirene Bureaux' workload can be best achieved through each Sirene Bureau having a computerised management system (workflow system), which allows a great deal of automation in the management of the daily workflow.

The Sirene Bureau may have a back-up computer and database system for its workflow at a secondary site in case of a serious emergency at the Sirene Bureau. This should include sufficient back-up power and communication supply.

Appropriate IT support should be provided for Sirene workflow to ensure its high availability.

1.13. **Time limits for response**

The Sirene Bureau shall answer all requests for information on alerts and hit procedures, made by the other Member States via their Sirene Bureaux, as soon as possible. In any event a response shall be given within 12 hours. (See also Section 1.13.1 on indication of urgency in Sirene forms.)

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

▼ **M1**1.13.1. *Indication of urgency in Sirene forms including urgent reporting of a hit*

Sirene forms to be dealt with by the requested Sirene Bureau with highest priority may be marked 'URGENT', in field 311 ('Important Notice'), followed by the reason for urgency. The reason for urgency shall be explained in the appropriate fields of the Sirene forms. Telephone communication or notification may also be used where an urgent response is required.

Where the circumstances of a hit on an alert dictate, such as a case of genuine urgency or significant importance, 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**.

1.14. **Transliteration/transcription rules**

The transliteration and transcription definitions and rules are set out in Appendix 1. They shall be respected in the communication between Sirene Bureaux (see also Section 2.10 on entering proper names).

1.15. **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 should have the necessary national competence to perform this role. Therefore, an adequate form of national data quality audit should 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 coordinator, the necessary IT support and appropriate rights within the systems should be available.

National standards for training users on data quality principles and practice should be established in cooperation with the national Sirene Bureau. Member States may call upon the staff of the Sirene Bureaux to be involved in the training of all authorities entering alerts, stressing data quality and maximisation of the use of SIS II.

1.16. **Archiving**

- (a) Each Member State shall establish conditions for storing information.
- (b) The Sirene Bureau of the issuing Member State shall keep all 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.

▼ **M1**

- (d) In accordance with Article 12(4) of the SIS II legal instruments 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 SIS II, and in any event at the latest one year thereafter. However, data relating to a particular alert which a Member State has entered 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 laws in the recipient Member State. Common Article 12 of the SIS II legal instruments, the Directive 95/46/EC and Framework Decision 2008/977/JHA also apply.
- (f) Information on misused identity shall be deleted after the deletion of the relevant alert.
- (g) Access to archives shall be recorded, controlled and restricted to designated staff.

**1.17. Staff**

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 desirable, which requires the unambiguous support of management to create a devolved working environment. Member States are encouraged to take appropriate measures to avoid loss of qualification and experience caused by staff turnover.

**1.17.1. Heads of Sirene Bureaux**

The Heads of Sirene Bureaux should 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. The meeting of the Heads of Sirene Bureaux is organised by the Member State holding the Presidency of the Council of the European Union.

**1.17.2. Sirene Contact Person (SIRCoP)**

In cases where standard procedures may be insufficient, the Sirene Contact Person (SIRCoP) may deal with files on which progress is complex, problematic or sensitive and a degree of quality assurance and/or longer term contact with another Sirene Bureau may be required in order to resolve the issue. The SIRCoP is not intended for urgent cases where the 24/7 front desk services shall in principle be used.

The SIRCoP may formulate proposals to enhance quality and describe options to resolve such issues in the longer term.

As a general rule SIRCoP are contactable by another SIRCoP only during office hours.

▼ **M1**

An annual assessment shall be carried out within the framework of the annual statistical reporting as it is set out in Appendix 5 based upon the following indicators:

- (a) number of SIRCoP interventions per Member State;
- (b) reason for contact;
- (c) result of the interventions based on information available during the reporting period.

1.17.3. *Knowledge*

Sirene Bureau staff shall have linguistic skills covering as wide a range of languages as possible and on-duty staff shall be 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.

1.17.4. *Training***National level**

At the national level, sufficient training shall ensure that staff meet 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.

The delivery of training should be in compliance with the Sirene Trainers Manual.

▼ **M1**

Article 3 of Regulation (EU) No 1077/2011 of the European Parliament and of the Council <sup>(1)</sup> sets out that the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (the Agency) shall perform tasks relating to training on the technical use of SIS II, in particular for Sirene staff.

1.17.5. *Exchange of staff*

As far as possible, Sirene Bureaux should 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.

## 2. GENERAL PROCEDURES

The procedures described below are applicable to all categories of alerts. 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 which entered the alert in SIS II;

‘Executing Member State’: Member State which takes the required actions following a hit;

‘Providing Sirene Bureau’: Sirene Bureau of a Member State which has fingerprints or pictures of the person for whom an alert was entered by another Member State.

‘Hit’: a hit occurs in SIS II when:

- (a) a search is conducted by a user,
- (b) the search reveals a foreign alert in SIS II,
- (c) data concerning the alert in SIS II matches the search data, and
- (d) further actions are requested as a result of the hit

‘Flag’: a suspension of validity at the national level 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 on the basis of the alert shall not be taken on the territory of this Member State.

<sup>(1)</sup> Regulation (EU) No 1077/2011 of 25 October 2011 of the European Parliament and of the Council establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).



▼ **M1****2.2. Multiple alerts (Article 34(6) of the SIS II Regulation and Article 49(6) of the SIS II Decision)**

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

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

Several alerts may be entered by different Member States for the same subjects. It is essential that this does not cause confusion to 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 in SIS II.

This calls for:

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

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

**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 — immediate action	Alert for specific check	Alert for discreet check — immediate action	Alert for discreet check	Alert on missing person (whereabouts)	Alert for judicial procedure
Alert for arrest	yes	yes	yes	no	no	no	no	yes	yes
Alert for refusal of entry	yes	yes	no	no	no	no	no	no	no
Alert on missing person (protection)	yes	no	yes	no	no	no	no	yes	yes
Alert for specific check — immediate action	no	no	no	yes	yes	no	no	no	no
Alert for specific check	no	no	no	yes	yes	no	no	no	no
Alert for discreet check — immediate action	no	no	no	no	no	yes	yes	no	no

▼ **M1**

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

**Table of compatibility for alerts on objects**

Order of importance	Alert for use as evidence	Document invalidated for travel purposes	Alert for seizure	Alert for specific check — immediate action	Alert for specific check	Alert for discreet check — immediate action	Alert for discreet check
Alert for use as evidence	yes	yes	yes	no	no	no	no
Document invalidated for travel purposes	yes	yes	yes	no	no	no	no
Alert for seizure	yes	yes	yes	no	no	no	no
Alert for specific check — immediate action	no	no	no	yes	yes	no	no
Alert for specific check	no	no	no	yes	yes	no	no
Alert for discreet check — immediate action	no	no	no	no	no	yes	yes
Alert for discreet check	no	no	no	no	no	yes	yes

**2.2.2. Order of priority of alerts**

In case of incompatible alerts the order of priority for alerts on persons shall be as follows:

— arrest with a view to surrender or extradition (Article 26 of Decision),

— refusing entry or stay in the Schengen territory (Article 24 of Regulation),

— placing under protection (Article 32 of Decision),

— specific check — immediate action (Article 36 of Decision),

— specific check (Article 36 of Decision),

▼ **M1**

- discreet check — immediate action (Article 36 of Decision),
- discreet check (Article 36 of 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 of document invalidated for travel purposes (Article 38 of Decision),
- seizure (Article 38 of Decision),
- specific check — immediate action (Article 36 of Decision),
- specific check (Article 36 of Decision),
- discreet check — immediate action (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.

### 2.2.3. *Checking for incompatibility and entering multiple alerts*

In order to avoid incompatible multiple alerts, it is important 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 Sirene Bureau shall ensure that only one alert exists in SIS II in accordance with national procedure if a request for an alert conflicts with an alert entered by the same Member State.

The following procedure shall apply in order to verify if multiple alerts exist on the same person or same object:

(a) The mandatory identity description elements shall be compared when establishing the existence of multiple alerts:

(i) on a person:

- surname,
- forename,
- date of birth,
- sex;

(ii) on a vehicle:

- the VIN,
- the registration number and country of registration,

**▼ M1**

— the make,

— the type;

(iii) on an aircraft:

— category of aircraft,

— ICAO registration number;

(iv) on a boat:

— category of boat,

— number of hulls,

— boat external identification number (not mandatory but may be used);

(v) on a container:

— BIC number <sup>(1)</sup>.

(b) When entering a new alert on a vehicle or other object with a VIN or registration number see procedures in Section 8.2.1.

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

The procedures described in Section 8.2.1 (checking for multiple alerts on a vehicle) shall be used to distinguish between other categories of objects in SIS II when it becomes apparent that two similar objects have the same serial number.

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 <sup>(2)</sup>.

If the check for multiple alerts reveals that the details are identical and relate to the same person or object, the Sirene Bureau of the Member State which intends to enter a new alert shall consult the Sirene Bureau of the issuing Member State if the alerts are incompatible.

The following procedure shall apply to verify the compatibility of alerts:

<sup>(1)</sup> Certain transportation companies use other reference numbers. SIS II has a provision for entering serial numbers other than the BIC.

<sup>(2)</sup> Due to the lack of standardisation in serial numbers for objects it is possible, for example, for two different firearms of different makes to have the same serial number. Equally it is possible for an object to have the same serial number as a very different object, for example, an issued document and a piece of industrial equipment. Where it is clear that the serial numbers are identical but the objects are clearly not the same no consultation between Sirene Bureaux is required. Users may be made aware that this situation can arise. Additionally, it is possible that an object, such as a passport or car, has been stolen and reported in one country and is subsequently reported in the country of origin. This could result in two alerts for the same object. If this matter comes to light it may be resolved by the Sirene Bureaux concerned.

▼ **M1**

- (a) prior to entering an alert it is mandatory to carry out a check to ensure that there are no incompatible alerts;
- (b) if another alert exists which is compatible, the Sirene Bureaux do not need to consult one another. However, if there is a need to clarify whether the alert relates to the same person the Sirene Bureau shall consult the Sirene Bureau of the issuing Member State using the **L form**;
- (c) if the alerts are incompatible, the Sirene Bureaux shall consult one another using an **E form** so that ultimately only one alert is entered;
- (d) alerts for arrest shall be entered immediately without awaiting the result of any consultation with other Member States;
- (e) 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 the Sirene Bureaux;
- (f) 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;
- (g) 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.

#### 2.2.4. *Special situation of the United Kingdom and Ireland*

The United Kingdom and Ireland do not take part in the SIS II Regulation therefore they cannot access the alerts on refusal of entry or stay (Articles 24 and 26 of the SIS II Regulation). They shall, nevertheless, be bound by the rules on compatibility of alerts as set out in Section 2.2 and in particular they shall apply the procedure referred in Section 2.2.3.

The following procedure shall apply:

- (a) Should the United Kingdom or Ireland enter an alert which is potentially incompatible with an existing alert on refusal of entry or stay in accordance with Section 2.2.1 the Central SIS II notifies these two Member States on the potential incompatibility by communicating only the Schengen ID of the existing alert.
- (b) Should an alert inserted by the United Kingdom or Ireland be notified of a potential incompatibility with an alert on refusal of entry or stay entered by another Member State, the Sirene Bureau of the United Kingdom or Ireland shall initiate a consultation with the issuing Member State by using free text message and shall delete the potentially incompatible alert during the consultation.
- (c) Depending on the outcome of the consultation the United Kingdom or Ireland can reinsert an alert which has been shown to be compatible.

▼ **M1****2.3. The exchange of information after a hit**

If the user requires supplementary information after a hit, the Sirene Bureau shall contact the Sirene Bureau of the issuing Member State without delay and request 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 (see also Section 1.13.1 on indication of urgency)

The following procedure shall apply:

- (a) Without prejudice to Section 2.4 of this Manual, one hit on an individual or an object for which an alert has been entered, shall in principle be communicated to the Sirene Bureau of the issuing Member State using one **G form**.
- (b) When notifying the issuing Member State of a hit, the applicable article of the SIS II legal instruments shall be indicated in field 090 of the **G form**, including additional information if necessary (e.g. MINOR).

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

- (c) If the Sirene Bureau of the executing Member State intends to provide further information after a **G form** has been sent, it shall use an **M form**.
- (d) If necessary, the Sirene Bureau of the issuing Member State shall then send any relevant, specific information and indicate any particular measures that it requests the Sirene Bureau of the executing Member State to take.

For the reporting procedure on hits achieved via Automatic Number Plate Recognition (ANPR) systems see Section 9.

**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, which is on the basis of all available information definitely unable to follow the procedure, shall inform the issuing Member State via its Sirene Bureau that it is not able to perform the requested action, and give the reasons in field 083 of an **H form**;
- (b) the Member States concerned may agree on the action to be taken in line with their own national laws and the SIS II legal instruments.

▼ **M1****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 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 they were 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 intends to process data in SIS II for a purpose other than that for which they were entered, the exchange of information shall take place according to the following rules:

- (a) through its Sirene Bureau, the Member State that intends to use data for a different purpose shall explain to the Member State that entered 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 request can be met and inform the other Member State by using an **M form**, through its Sirene Bureau, of its decision;
- (c) if need be, the Member State that entered the alert may grant authorisation subject to certain conditions on how the data are to be used. This authorisation shall be sent by using an **M form**.

Once the Member State that entered the alert has agreed, the other Member State shall only use the data for the purpose for which it obtained authorisation. It shall take account of any conditions set by the issuing Member State.

**2.6. Flagging****2.6.1. Introduction**

- (a) Article 24 of the SIS II Decision provides for the following cases where a Member State may require a flag:
  - (i) Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 or 36 of the SIS II Decision is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added by the Sirene Bureau of the issuing Member State.
  - (ii) In order to enable Member States to require that a flag be added to an alert issued in accordance with Article 26, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.

▼ **M1**

- (iii) If in particularly urgent and serious cases, a Member State issuing an alert requests the execution of the action, the Member State executing the alert shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the Member State executing the alert is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.
- (b) An alternative procedure exists only for alerts for arrest (see Section 3.6).
- (c) When a flag is added to alerts for missing persons and alerts for discreet or specific checks the alert does not appear on the screen when the user consults the system.
- (d) Without prejudice to Section 3.6.1 a Member State shall not request a flag solely on the basis that a given Member State is the issuing Member State. Flags shall only be requested on a case-by-case basis.

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

A flag shall be added **only** at the request or agreement of another Member State.

The following procedure shall apply:

- (a) If a Member State requests a flag to be added, it shall request the flag from the issuing Member State using an **F form**, explaining the reason for the flag. Field 071 shall be used for this purpose, explaining in field 080 the reason for the flag. For other supplementary information concerning the alert field 083 shall be used.
- (b) The Member State that entered the alert shall add the requested flag immediately.
- (c) Once information has been exchanged, based on the information provided for in the consultation process by the Member State requesting the flag, the alert may need to be amended or deleted or the request may be withdrawn, leaving the alert unchanged.

2.6.3. *A request for deletion of a flag*

Member States shall request the deletion of the previously requested flag as soon as the reason for the flag is no longer valid. This may be the case, in particular, if national legislation has changed or if further information exchange about the case reveals that the circumstances referred to in Article 24(1) or 25 of the SIS II Decision no longer exist.

The following procedure shall apply:

- (a) The Sirene Bureau which previously requested the flag to be added shall request the Sirene Bureau of the issuing Member State to delete the flag, using an **F form**. Field 075 shall be used for this purpose<sup>(1)</sup>. For more details concerning national law field 080 shall be used and, where appropriate, for inserting supplementary information explaining the reason for the deletion of the flag and for other supplementary information concerning the alert field 083 shall be used.

<sup>(1)</sup> For the technical implementation see the Data Exchange between Sirenes document referred to in Section 1.10.2.



▼ **M1**

- (b) The Sirene Bureau of the issuing Member State shall delete the flag immediately.

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 Article 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.

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

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

Without prejudice to national law, when the national authorities need 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 law on the right to access personal data. Depending on the circumstances of the case and in accordance with the applicable law, 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 competent national authorities so require, 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*

Information on requests for access to alerts entered in SIS II by another Member State shall be exchanged via the national Sirene Bureaux using a **K form** for persons or an **M form** for objects.

The following procedure shall apply:

- (a) the request for access shall be forwarded to the Sirene Bureau of the issuing Member State as soon as possible, so that it can take a position on the question;

▼ **M1**

- (b) the Sirene Bureau of the issuing Member State shall inform the Sirene Bureau of the Member State that received the request of access of its position;
- (c) the response by the Sirene Bureau of the issuing Member State shall take into account any deadlines for processing the request set by the Sirene Bureau of the Member State that received the request for access;
- (d) the Sirene Bureau of the Member State receiving an enquiry from an individual for access, correction or deletion shall take all the necessary measures to ensure a timely response.

If the Sirene Bureau of the issuing Member State sends its position to the Sirene Bureau of the Member State that received the request for access, the Sirene Bureau, according to national law and within the limits of its competence, 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 entered the alert. If the person addresses a Member State other than the one that entered the alert, the Sirene Bureau of the requested Member State shall inform the Sirene Bureau of the issuing Member State by means of a **K form** and the procedure described in 2.8.2 shall apply.

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

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

As soon as the conditions for maintaining the alert are no longer fulfilled, the issuing Member State shall delete the alert without delay. When the alert has an expiry date, the deletion will occur automatically in the CS-SIS. In case of a hit, the particular procedures described in Sections 3.11, 4.10, 5.7, 6.5, 7.7 and 8.4 apply.

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.

2.10. **Entering proper names**

Within the constraints imposed by national systems for entry of data and availability of data, proper names (forenames and surnames) shall be entered in SIS II in a format (script and spelling) in the format used on official travel documents in accordance with the ICAO standards for travel documents, which are also used in the transliteration and transcription functionalities of Central SIS II. In the exchange of supplementary information, Sirene Bureaux shall use the proper names as they are entered in SIS II. Both users and Sirene Bureaux within the issuing Member States shall use, as a general rule, Latin characters for entering data in SIS II, without prejudice to transliteration and transcription rules laid down in Appendix 1.

▼ **M1**

Where it is necessary to exchange supplementary information on a person who is not subject of an alert but may be related to it (e.g. a person who may be accompanying a missing minor) then the presentation and spelling of the name shall follow the rules set out in Appendix 1 and be provided in Latin characters and original format, if the Member State providing the information has the capacity to also input any special characters in the original format.

## 2.11. **Different categories of identity**

### **Confirmed identity**

A confirmed 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, entered in SIS II, 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 Article 51 of the SIS II Decision)*

Due to the complexity of misused identity cases, on becoming aware that a person for whom an alert exists in 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.

Subject to the person's explicit consent, and as soon as it has been established that a person's identity has been misused, additional data shall be added to the alert in 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.

The issuing Member State is responsible for inserting the remark 'misused identity' in the alert and for entering additional data of the victim of misused identity such as photos, fingerprints and information on any valid ID document(s).

When a Member State discovers that an alert on a person entered by another Member State relates to a case of misused identity, and it has been established that the person's identity is misused it shall inform the Sirene Bureau of the issuing Member State using a **Q form**, in order that the misused identity extension can be used in the SIS II alert.

▼ **M1**

Taking into account the purpose for entering data of this nature, where the photographs and fingerprints of the person whose identity has been misused are available, they shall be added to the alert. For there to be a case of misused identity an innocent person's details must match an existing identity in an alert. The **Q form** must contain the identity details, including alias number, from the alert so that the issuing Member State may ascertain to which identity in the alert the form refers. The mandatory fields for completion of a **Q form** in such cases are set out in Appendix 3.

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, including any fingerprints and photographs, shall be deleted at the same time as the alert or earlier if the person concerned so requests.

2.11.2. *Entering an alias*

In order to avoid incompatible alerts of any category due to an alias to be entered, to avoid problems for innocent victims and 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 inform the issuing Member State 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 SIS II is insufficient, provide further information after consultation, on its own initiative or at the request of another Member State, to help clarify a person's identity. An **L Form** (and attachments) 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, date of issue, place and authority as well as the expiry date,
- description of the person sought,
- surname and forename of the mother and father of the person sought,
- other possible spellings of the surname and forenames of the person sought,
- photographs and fingerprints if available,
- last known address.

▼ **M1**

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**

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 SIS II and only this Member State may modify and delete the link. Links shall only be visible to users when they have correct user access rights which permit at least two alerts in the link to be visible to them. Member States shall ensure that only authorised access to links is possible.

### 2.12.1. *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 each of two or more interlinked alerts, the Sirene Bureau of the executing Member State shall send a **G form** for each of them indicating in field 086 that other **G forms** on the linked alerts will be forwarded.

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. However, if there is a linked alert for surrender/extradition or for a missing person (for their own protection or in order to prevent threats) the communication of this discovery shall be carried out using an **M form** if appropriate and the information is available.

## 2.13. **Format and quality of biometric data in SIS II**

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.

Sirene Bureaux shall be able to exchange fingerprints and pictures for the purpose of completing the alert and/or to support the execution of the requested action to be taken. 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 as an attachment in order to allow the issuing Member State to complete the alert.

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

▼ **M1**2.13.1. *Further use of the data exchanged, including archiving*

Limitations on the use of data provided for alerts in SIS II are set out in the SIS II legal instruments. Any further use of pictures and fingerprints exchanged, including archiving, shall comply with the relevant provisions of the SIS II legal instruments, applicable national provisions on data protection, in accordance with Directive 95/46/EC and Framework Decision 2008/977/JHA.

Any storage of fingerprints at the national level shall fully respect the data protection rules of SIS II. Member State shall keep fingerprint data downloaded from CS-SIS separately from national fingerprint databases and such data shall be deleted at the same time as corresponding alerts and supplementary information.

2.13.2. *Exchanging fingerprints and photographs*

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 an **L form** that the fingerprints and pictures are being sent to complete an alert in SIS II;
- (b) the Sirene Bureau of the issuing Member State shall add the fingerprints or pictures to the alert in SIS II or shall send them to the competent authority to complete the alert.

2.13.3. *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 SIS II.

Every Sirene Bureau shall fulfil those technical standards.

2.13.4. *Format and quality of biometric data*

All biometric data entered in the system shall be subject of 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:

- (a) fingerprint data is compliant with the ANSI/NIST — ITL 1-2000 specified format, as implemented for the purposes of Interpol and adapted for SIS II;
- (b) 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 ratio 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 KB.

▼ **M1**2.14. **Special types of search**2.14.1. *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 person or object, subject of an alert, within a restricted geographical area.

Geographically targeted searches in the Schengen area shall take place on the basis of an alert in SIS II. In circumstances where the whereabouts of a person or object are known, field 311 (Important Notice) may be completed indicating a geographical search and selecting the appropriate countries. Additionally, if the whereabouts are known when issuing an alert for arrest, field 061 of an **A Form** shall include the information on whereabouts of the wanted person. In all other cases, including for communicating the whereabouts of objects, an **M form** (field 083) shall be used. An alert for the wanted person shall be entered in SIS II to ensure that a request for action to be taken is immediately enforceable (Article 9(3) of the Council Framework Decision 2002/584/JHA <sup>(1)</sup>).

When the subject of a geographical search is located at a place other than that indicated in the geographical search the Sirene Bureau of the issuing Member State shall indicate this fact, using an **M form**, to the Member State(s) involved in the geographical search in order for any related work to be stopped.

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

The services provided by special units that conduct targeted searches (*Fugitive, Active Search Teams*, FAST) should also be used in suitable cases by Sirene Bureaux in the requested Member States. The alert in SIS II should not be replaced by international cooperation of the above-mentioned police units. Such cooperation should not overlap the Sirene Bureau's role as a focal point for searches using SIS II.

Cooperation, as appropriate, should be established to ensure that the Sirene Bureau of the issuing Member State is informed by their national FAST about any ongoing operation relating to an alert entered in SIS II. Where appropriate this Sirene Bureau shall provide this information to other Sirene Bureaux. Any coordinated operation of Enfast (European Network of Fugitive Active Search Teams) which entails the cooperation of the Sirene Bureau shall be reported in advance to the Sirene Bureau.

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

<sup>(1)</sup> Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

**▼ M1****3. ALERTS FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES (ARTICLE 26 OF THE SIS II DECISION)****3.1. Entering an alert**

Most of the alerts for arrest are accompanied by a European Arrest Warrant (EAW). However, under an alert for arrest, a provisional arrest is also possible prior to obtaining a request for extradition (ER) according to Article 16 of the European Convention on Extradition.

The EAW/ER shall be issued by a competent judicial authority carrying 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 in SIS II. A translation of the EAW in one or more of the official languages of the institutions of the Union 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 issuing Member State to delete an EAW that loses its validity and to check if there are any other EAWs attached to the alert and extend the alert if needed.

In addition to an EAW which a Member State has attached to an alert for arrest it shall also be possible to attach translations of the EAW, if necessary in separate binary files.

For scanned 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. The Sirene Bureau of the executing Member State shall send a **G form** to each Member State concerned.

**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.



▼ **M1**

In the case of alerts for arrest, the Sirene Bureau shall use field 011 of an **A form** <sup>(1)</sup> (at the time of entry of the alert) or subsequently an **M form**, when informing the other Member States of aliases regarding an alert for arrest, if this information is available to the Sirene Bureau.

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

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

The information referred to in Section 3.5.1 shall be sent to the other Sirene Bureaux by **A form**, at the same time as entering the alert. 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’, fields 042, 043, 044, 045: ‘description of the circumstances’) for other Sirene Bureaux to verify the alert. Appendix 3 sets out the information required and its relation to the fields on the EAW.

When an EAW is replaced or revoked this shall be indicated in field 267 of an **A form** (Article 26 SIS II Decision) or in field 044 of an **A form** (Extradition Request/Migrated alerts) by using the following text: ‘This form replaces the form (reference number) referring to EAW (reference number) issued on (date)’.

#### 3.5.1. *Supplementary information to be sent with regard to provisional arrest*

##### 3.5.1.1. When entering an alert based on both an EAW and an extradition request (ER)

When entering 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.

##### 3.5.1.2. When issuing an alert based on ER only

When entering 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 attached to the alert can be executed, the alert shall not be flagged.

<sup>(1)</sup> For the technical implementation see the Data Exchange between Sirenes document referred to in Section 1.10.2.

▼ **M1**

If an EAW contains more than one offence and if surrender can be carried out in respect of at least one of those offences, the alert shall not be flagged.

As highlighted in Section 2.6, a flagged alert under Article 26 of the SIS II Decision shall, for the period of duration of the flag, be regarded as being entered for the purposes of communicating the whereabouts of the person for whom it was issued.

3.6.1. *Systematic request for a flag to be added to alerts on persons wanted for arrest for extradition purposes where Framework Decision 2002/584/JHA does not apply*

The following procedure shall apply:

- (a) in the case of alerts on persons wanted for arrest for extradition purposes, where Framework Decision 2002/584/JHA does not apply, a Sirene Bureau may ask other Sirene Bureau(x) to add a flag systematically to alerts entered under Article 26 of the SIS II Decision on its nationals;
- (b) any Sirene Bureau wishing to do so shall send a written request to other Sirene Bureau(x);
- (c) any Sirene Bureaux to whom such a request is addressed shall add a flag for the Member State in question immediately after the alert is issued;
- (d) the flag shall remain until the requesting Sirene Bureau asks for its deletion.

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 to 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. The receiving Member States shall carry out searches to the extent permissible under national law.

If the alert for arrest is verified and the subject is located or arrested in a Member State, then the information contained in an **A form** may be forwarded by the receiving Sirene Bureau to the competent authority of the Member State which executes the EAW or the ER. If the original EAW or ER is requested, the issuing judicial authority may transmit it directly to the executing judicial authority (unless alternative arrangements have been made by the issuing and/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 shall always be communicated immediately to the Sirene Bureau of the issuing Member State. Moreover, after sending a **G form** the Sirene Bureau of the executing Member State shall also communicate the hit to the Sirene Bureau of the issuing Member State where appropriate by telephone;

▼ **M1**

- (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;
- (c) the authority competent for receiving the EAW or ER, its full communication contacts (postal address, phone and, if available, fax and e-mail), reference number (if available), competent person (if available), requested language, time limit for and form of delivery shall be provided in field 091 of a **G form**;
- (d) in addition, the Sirene Bureau of the issuing Member State shall inform other Sirene Bureaux of the hit, using an **M form**, where a clear link has been established with particular Member States from the facts of the case and further enquiries initiated;
- (e) the Sirene Bureaux may transmit further information on alerts under Article 26 of the SIS II Decision, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance.

### 3.9. **Supplementary information exchange about surrender or extradition**

When the competent judicial authorities provide information to the Sirene Bureau of the executing Member State on whether the surrender or extradition may take place of a person for whom an alert for arrest has been issued, that Sirene Bureau shall immediately provide that information to the Sirene Bureau of the issuing Member State by means of an **M form**, marked in field 083 with the words 'SURRENDER' or 'EXTRADITION' <sup>(1)</sup>. The detailed arrangements of the surrender or extradition shall, where appropriate, be communicated via the Sirene Bureaux as soon as possible.

### 3.10. **Supplementary information exchange about transit through another Member State**

If the transit of a person is necessary, the Sirene Bureau of the Member State through which the person is to be taken shall provide the necessary information and support, in response to a request by the Sirene Bureau of the issuing Member State or the competent judicial authority, sent by the Sirene Bureau, by means of an **M form** marked with the word 'TRANSIT' written at the start of field 083.

### 3.11. **Deletion of alerts upon surrender or extradition**

Deletion of alerts for arrest for surrender or extradition purposes shall take place once the person has been surrendered or extradited to the competent authorities of the issuing Member State but may also occur when the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.

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

### **Introduction**

The exchange of information on third-country nationals on whom an alert has been issued under Article 24 of the SIS II Regulation allows Member States to take decisions in the case of entry or visa application. If the individual is already on the territory of the Member State, it allows

<sup>(1)</sup> See also Section 1.13.1 on indication of urgency in Sirene forms.

▼ **M1**

national authorities to take the appropriate action for issuing residence permits, long-stay visas or expulsion. In this section references to visas concern long-stay visas, unless otherwise clearly explained (e.g. re-entry visa).

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

Directive 2004/38/EC of the European Parliament and of the Council <sup>(1)</sup> is not applicable in Switzerland. Therefore in the case of hit on a third country national who is the beneficiary of the right of free movement, normal consultation procedures shall be undertaken between Switzerland, the issuing Member State and any other Member State which may hold relevant information on the third country national's right of free movement.

#### 4.1. **Entering an alert**

According to Article 25 of the SIS II Regulation, specific rules apply to third-country nationals who are beneficiaries of the right of free movement within the meaning of Directive 2004/38/EC. 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 was entered for a beneficiary of the right of free movement <sup>(2)</sup>. In the exceptional case of entry of an alert on a third-country national enjoying the right of free movement, the Sirene Bureau of the issuing Member State shall send an **M form** to all the other Member States, based on the information provided by the authority that has entered the alert (see Sections 4.6 and 4.7)

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 29 of the Treaty on European Union <sup>(3)</sup>, shall also be entered. The alerts shall be entered and kept up-to-date by the competent

<sup>(1)</sup> 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 (OJ L 158, 30.4.2004, p. 77).

<sup>(2)</sup> 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.

<sup>(3)</sup> Article 26 of the SIS II Regulation refers to Article 15 of the Treaty on European Union. However, following the entry into force of the Lisbon Treaty this Article 15 became Article 29 in the consolidated version of the Treaty on European Union.

▼ **M1**

authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS II or alerts under Article 24 of the SIS II Regulation the responsibility shall be taken up by the Member State which will hold the subsequent Presidency and has access to SIS II, including access to the alerts under Article 24 of the SIS II Regulation.

Member States shall put in place the necessary procedures for entering, updating and deleting such alerts.

#### 4.2. **Multiple alerts**

See general procedure in Section 2.2.

#### 4.3. **Misused identity**

See general procedure in Section 2.11.1.

Problems may occur when a third country national who is subject of an alert for refusal of entry or stay unlawfully uses the identity of a citizen of a Member State in order to seek to gain entry. If such a situation is discovered the competent authorities in the Member States may be made aware of the correct use of the misused identity function within SIS II. Alerts for refusal of entry shall not be issued in the main identity of a citizen of a Member State.

#### 4.4. **Entering an alias**

For general rules see Section 2.11.2.

#### 4.5. **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 Section 4.8, which concerns the exchange of information following a hit on a third-country national who is the beneficiary of the 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 issuing Member that the alert for refusal of entry has been matched in the course of the procedure for granting a residence permit or a visa. The issuing Member State may then inform other Member States using an **M form** if appropriate;
- (b) if so requested, in accordance with national law, the Sirene Bureaux of the Member States concerned may assist in transmitting the necessary information to the appropriate authorities responsible for granting 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 or visa discovers that the applicant concerned is the subject of an alert for refusal of entry or stay issued by another Member State, it shall consult the issuing Member State via the Sirene Bureaux. The Member

▼ **M1**

State considering granting a residence permit or visa shall use an **N form** to inform the issuing Member State about the decision to grant the residence permit or visa. If the Member State decides to grant the residence permit or visa, the alert shall be deleted. The person may, nevertheless, be put on the issuing 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 granted a residence permit or visa, it shall instigate a consultation procedure with the Member State that granted the residence permit or visa, via the Sirene Bureaux. The Member State which granted the residence permit or visa shall use an **O form** to inform the issuing Member State about the decision whether or not to withdraw the residence permit or visa. If this Member State decides to maintain the residence permit or visa, the alert shall be deleted. The person can, nevertheless, be put on a Member State's national list of alerts for refusal of entry.

The consultation via Sirene Bureaux using an **O form** shall also take place if the Member State that granted the residence permit or visa discovers later that there is an alert for refusal of entry or stay on that person entered in SIS II <sup>(1)</sup>.

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

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

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

##### 4.5.1. 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, long stay visa or a re-entry visa granted by one of the Member States, shall be allowed entry for transit purposes to the Member State which granted the residence permit or re-entry visa, when crossing a border in a third Member State. The entry may be refused if this Member State has issued a national alert for

<sup>(1)</sup> 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 Member State only regarding any previous police record (that is not all of the SIS II data). Such enquiries shall not be made as a matter of routine.

▼ **M1**

refusal of entry. In both cases, at the request of the competent authority, the Sirene Bureau of the Member State that the person is seeking to enter shall send the Sirene Bureaux of the two Member States in question a message (an **H form** if the transit was allowed/a **G form** if the entry was refused) informing them of the contradiction and requesting that they consult each other in order to either delete the alert in SIS II or to withdraw the residence permit/visa. It may also request to be informed of the result of any consultation.

If the third-country national concerned tries to enter the Member State which has entered the alert in 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 granted the residence permit or visa in order to allow the competent authority to determine whether there are sufficient reasons for withdrawing the residence permit/visa. The Member State which granted the residence permit or visa shall use an **O form** to inform the issuing Member State about the decision whether or not to withdraw the residence permit or visa. If this Member State decides to maintain the residence permit or visa, the alert shall be deleted. The person can, nevertheless, be put on a Member State's national list of alerts for refusal of entry.

If this person tries to enter the Member State that issued the residence permit or visa, 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 consult the Sirene Bureau of the issuing Member State in order to enable the competent authorities concerned to decide on withdrawal of the residence permit or visa or deletion of the alert. The Member State which granted the residence permit or visa shall use an **O form** to inform the issuing Member State about the decision whether or not to withdraw the residence permit or visa. If this Member State decides to maintain the validity of the residence permit or visa, the alert shall be deleted. The person can, nevertheless, be put on a Member State's national list of alerts for refusal of entry.

#### 4.5.2. *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 the Sirene Bureau of the issuing Member State of this situation using an **H form**.

#### 4.6. **Common rules concerning procedures referred to in Section 4.5**

- (a) Only one **N form** or **O form** shall be sent per consultation procedure by the Sirene Bureau of the Member State which has granted or intends to grant or retain a residence permit or long-stay visa in order to inform the Member State which has issued or is planning to issue a refusal of entry alert about the final decision on granting, retaining or revoking the residence permit or visa.
- (b) The consultation procedure shall be either a procedure for the purposes of Article 25(1) of the Schengen Convention or a procedure for the purposes of Article 25(2) of the Schengen Convention.

▼ **M1**

- (c) When a **M**, **G** or **H form** is sent in the context of a consultation procedure, it may be marked with the keyword 'consultation procedure'. (**M form**: field 083; **G form**: field 086; **H form**: field 083).

#### 4.7. **Exchange of information following a hit and when refusing entry or expelling from the Schengen area**

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 Section 4.8 which concerns the exchange of information following a hit on a third-country national who is the beneficiary of the 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 entered.

The Sirene Bureaux of Member States that have entered 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** or an **H form**, depending on the action taken, 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 right of free movement.

Notwithstanding the provisions of the paragraph above, as set out in Section 10 all Sirene Bureaux shall provide statistics on hits on all foreign alerts on their territory.

The following procedure shall apply:

- (a) A Member State may ask to be informed of any hits on alerts for refusal of entry or stay that it has issued. Any Member State that wishes to take up this option shall ask the other Member States in writing.
- (b) The executing Member State may take the initiative and inform the issuing Member State that the alert has been matched and that the third-country national has not been granted entry or has been expelled from the Schengen territory.
- (c) Once an action has been taken on the basis of a hit the Sirene Bureau of the executing Member State shall send a **G form** to the Sirene Bureau of the issuing Member State; a **G form** shall also be sent in case of a hit, when more information is needed for the execution of the measure.
- (d) Upon the receipt of the information referred to in point (c) from the issuing Member State:
  - (i) if the action is executed the executing Member State shall notify the Sirene Bureau of the issuing Member State using an **M form** (not another **G form** for the same hit),
  - (ii) if the action is not executed the executing Member State shall notify the Sirene Bureau of the issuing Member State using an **H form**, or



▼ **M1**

- (iii) if further consultation is required this shall take place using an **M form**,
- (iv) for the final form exchange in a consultation procedure an **N** or **O form** shall be used.
- (e) If, on its territory, a Member State discovers a third-country national for whom an alert has been issued, the Sirene Bureau of 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 this information, given in an **M form**, shall include the following:
  - the type and reason for the decision,
  - the authority issuing the decision,
  - the date of the decision,
  - the date of service (the date on which the decision was served),
  - the date of enforcement,
  - the date on which the decision expires or the length of validity,
  - the information whether the person was convicted and the nature of the penalty.

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 may also be an urgent need for supplementary information to be exchanged via the Sirene Bureaux in specific cases in order to identify an individual with certainty.

#### 4.8. **Exchange of information following a hit on a third-country national who is a beneficiary of the right of free movement**

Concerning a third-country national who is a beneficiary of the right of free movement within the meaning of Directive 2004/38/EC <sup>(1)</sup>.

If there is a hit on a third-country national who is beneficiary of the right of free movement within the meaning of Directive 2004/38/EC special rules shall apply (but see the introduction to Section 4 on the position of Switzerland). The following procedure shall apply:

<sup>(1)</sup> According to Directive 2004/38/EC, a person benefiting from the right of free movement may only be refused entry or stay on the grounds of public policy or public security when their personal conduct represents a genuine, immediate, and sufficiently serious threat affecting one of the fundamental interests of society and when the other criteria laid down in Article 27(2) of the said Directive are respected. Article 27(2) stipulates: 'Measures taken on grounds of public policy or public security shall comply with the principle of proportionality and shall be based exclusively on the personal conduct of the individual concerned. Previous criminal convictions shall not in themselves constitute grounds for taking such measures. The personal conduct of the individual concerned must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society. Justifications that are isolated from the particulars of the case or that rely on considerations of general prevention shall not be accepted.' Moreover, there are additional limitations for persons enjoying the right of permanent residence who can only be refused entry or stay on serious grounds of public policy or public security as stated in Article 28(2) of Directive 2004/38/EC.

▼ **M1**

- (a) at the request of the competent authority, the Sirene Bureau of the executing Member State shall immediately contact the Sirene Bureau of the issuing Member State using a **G form** in order to obtain the information necessary to decide, without delay, on the action to be taken;
- (b) upon receipt of a request for information, the Sirene Bureau of the issuing Member State shall immediately start gathering the required information and send it as soon as possible to the Sirene Bureau of the executing Member State;
- (c) the Sirene Bureau of the issuing Member State shall check with the competent authority, if this information is not yet available, whether the alert may be kept in accordance with Directive 2004/38/EC. If the competent authority decides to keep the alert, the Sirene Bureau of the issuing Member State shall inform all the other Sirene Bureaux thereof, by means of an **M form**;
- (d) the executing Member State shall inform, via its Sirene Bureau, the Sirene Bureau of the issuing Member State whether the requested action to be taken was carried out (using an **M form**) or not (using an **H form**)<sup>(1)</sup>.

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

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

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

4.10. **Deletion alerts for refusal of entry or stay**

Without prejudice to the special procedures provided for by Article 25 of the Schengen Convention and Article 5(4)(a) and (c) of the Schengen Borders Code the alerts for refusal of entry or stay on third country nationals shall be deleted upon:

- (a) the expiry of the alert;
- (b) the decision to delete by the competent authority of the issuing Member State;
- (c) the expiry of the time limit on refusal of entry where the competent authority of the issuing Member State set an expiry date on its decision; or

<sup>(1)</sup> In conformity with Directive 2004/38/EC the executing Member State cannot limit the free movement of third country nationals benefiting from the right of free movement on the sole ground that the issuing Member State maintains the alert unless the conditions referred to in footnote 28 are met.

▼ **M1**

(d) the acquisition of citizenship of one of the Member States. If the acquisition of citizenship comes to the attention of a Sirene Bureau of a Member State other than the issuing one, the former shall consult the Sirene Bureau of the issuing Member State and, if needed, send 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)**

5.1. **Multiple alerts**

See general procedure in Section 2.2.

5.2. **Misused identity**

See general procedure in Section 2.11.1.

5.3. **Entering an alias**

See general procedure in Section 2.11.2.

5.4. **Adding a flag**

Circumstances may arise where a hit occurs on an alert on a missing person and the competent authorities within the executing Member State decide that the action requested may not be taken and/or that no further action will be taken on the alert. This decision may be taken even if the issuing Member State's competent authorities decide to retain the alert in SIS II. In such circumstances the executing Member State may request a flag after the 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.

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

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

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

▼ **M1**

- (a) retain the information in order to be able to forward supplementary information upon the request of another Member State;
- (b) forward an **M form** to the relevant Sirene Bureau if enquiries indicate a likely destination for the missing person;
- (c) forward an **M form** to all the relevant Sirene Bureaux, based on the disappearance circumstances for the purpose of supplying all data concerning the person in a short period of time.

In the case of a high-risk missing person, field 311 of the **M form** shall begin with the word 'URGENT' and an explanation of the reason for the urgency. (When the missing minor is unaccompanied <sup>(1)</sup>, the explanatory term 'Unaccompanied minor' shall be indicated.) This urgency may be reinforced by a telephone call highlighting the importance of the **M form** and its urgent nature.

A common method for entering structured supplementary information in an agreed order on a high-risk missing person shall be used <sup>(2)</sup>. This shall be entered in field 083 of the **M form**.

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

- (a) relevant border posts;
- (b) the competent administrative and police authorities for the location and protection of persons;

<sup>(1)</sup> Unaccompanied minors are children, as defined in Article 1 of the Convention on the Rights of the Child of 20 November 1989 (CRC), who have been separated from both parents and other relatives and are not being cared for by an adult who, by law or custom, is responsible for doing so.

<sup>(2)</sup> Data of disappearance:

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

(b) Circumstances of disappearance.

Details of the missing person:

(c) Apparent age.

(d) Height.

(e) Skin colour.

(f) Colour and shape of hair.

(g) Colour of eyes.

(h) Other physical details (i.e. piercings, deformations, amputations, tattoos, marks, scars, etc.).

(i) Psychological particulars: at risk of suicide, mental illness, aggressive behaviour, etc.

(j) Other details: necessary medical treatment, etc.

(k) Clothes worn at the time of the disappearance.

(l) Photograph: available or not.

(m) Ante-mortem form: available or not.

Related information:

(n) Person/s who could accompany him or her (and Schengen ID if available).

(o) Vehicle/s relating to the case (and Schengen ID if available).

(p) If available: number of mobile phone/last 'log-in', contact via on-line social networks.

The titles of the different sub-fields themselves are not to be included as part of field 083, but just the reference letter. When details are already available in the fields of an alert the information shall be included in the alert, including fingerprints or photographs.

▼ **M1**

- (c) the relevant consular authorities of the issuing Member State, after a hit is achieved in SIS II.

#### 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 communication of the whereabouts of the missing person, who is of age, to the person who reported him/her missing shall be subject to the missing person's consent <sup>(1)</sup>. The consent shall be in writing or at least a written record shall be available. In cases where consent is refused, this shall be in writing or recorded officially. 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.

#### 5.7. **Deletion of alerts on missing persons**

If there is to be any significant delay in the deletion of the alert by the issuing Member State this delay shall be notified to the Sirene Bureau of the executing Member State in order for a flag to be placed on the alert as described in Section 5.4 of the Sirene Manual.

##### 5.7.1. *Minors*

An alert shall be deleted upon:

- (a) the resolution of the case (e.g. the minor is repatriated; the competent authorities in the executing Member State take a decision on the care of the child);
- (b) the expiry of the alert; or
- (c) the decision by the competent authority of the issuing Member State.

##### 5.7.2. *Adults where no protective measures are requested*

An alert shall be deleted upon:

<sup>(1)</sup> For clarity on consent in matters of on the protection of individuals with regard to the processing of personal data and on the free movement of such data see Article 2(h) Directive 95/46/EC.

▼ **M1**

- (a) the execution of the action to be taken (whereabouts ascertained by the executing Member State);
- (b) the expiry of the alert; or
- (c) the decision by the competent authority of the issuing Member State.

5.7.3. *Adults, protective measures requested*

An alert shall be deleted upon:

- (a) carrying out of the action to be taken (person placed under protection);
- (b) the expiry of the alert; or
- (c) the decision by the competent authority of the issuing Member State.

Subject to national law, where a person is in official protective care an alert may be retained until that person has been repatriated.

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

6.1. **Multiple alerts**

See general procedure in Section 2.2.

6.2. **Misused identity**

See general procedure in Section 2.11.1.

6.3. **Entering an alias**

See general procedure in Section 2.11.2.

6.4. **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 law of the Member State where the person was located;
- (b) national procedures shall be in place, as appropriate, to ensure that alerts are only kept in SIS II for the time required to meet the purposes for which they were supplied.

The Sirene Bureaux may transmit further information on alerts entered under Article 34 of SIS II Decision, and in so doing may act on behalf of judicial authorities if this information falls within the scope of mutual judicial assistance.

6.5. **Deletion of alerts on persons sought for a judicial procedure**

An alert shall be deleted upon:

▼ **M1**

(a) the communication of the whereabouts of the person to the competent authority of the issuing Member State. Where the information forwarded cannot be acted upon (e.g. incorrect address or no fixed abode) the Sirene Bureau of the issuing Member State shall inform the Sirene Bureau of the executing Member State in order to resolve the problem;

(b) the expiry of the alert; or

(c) the decision by the competent authority of the issuing Member State.

Where a hit has been achieved in a Member State and the address details were forwarded to the issuing Member State and a subsequent hit in that Member State reveals the same address details the hit shall be recorded in the executing Member State but neither the address details nor a **G form** shall be re-sent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State on the repeated hits, and the issuing Member State shall consider the need to maintain the alert.

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

### 7.1. Multiple alerts

See general procedure in Section 2.2.

### 7.2. Misused identity

See general procedure in Section 2.11.1.

### 7.3. Entering an alias

See general procedure in Section 2.11.2.

### 7.4. Informing other Member States when issuing alerts

When issuing an alert the Sirene Bureau of the issuing Member State shall inform all the other Sirene Bureaux by using an **M form** in the following cases:

(a) an alert for discreet or specific check is issued with the request that hits are reported without any delay to the issuing Sirene Bureau; in the **M form** it shall use the text 'ARTICLE 36(2) of the SIS II Decision — immediate action' or 'ARTICLE 36(3) of the SIS II Decision — immediate action'. Justification for the immediate action should also be set out in field 083 of an **M form**; or

(b) an authority responsible for national security requests the issuance of an alert in accordance with Article 36(3) of the SIS II Decision; in the **M form** it shall use the text 'ARTICLE 36(3) of the SIS II Decision'.

If the alert is issued under Article 36(3) of the SIS II Decision the **M form** shall contain, in field 080, the name of the authority requesting entry of the alert, first in the language of the issuing Member State and then also in English and its contact details in field 081 in a format not requiring translation.

▼ **M1**

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

7.5. **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 authority responsible for national security in the executing Member State decides that the alert requires a flag, it shall contact its 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. As with other flag requests a general reason shall be given. However, matters of a sensitive nature need not be disclosed (see also Section 7.6(b) below).

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

See general procedure in Section 2.3.

In addition the following rules shall apply:

- (a) 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 (discreet check or specific check) via the **G form**. At the same time the Sirene Bureau of the executing Member State shall inform its own authority responsible for national security.
- (b) A specific procedure is required to safeguard the confidentiality of information. Therefore, any contact between the authorities responsible for national security shall be kept separate from the contact between the Sirene Bureaux. Consequently, the detailed reasons for requesting a flag shall be discussed directly between authorities responsible for national security and not through Sirene Bureaux.
- (c) When a hit occurs on an alert which requests the hit to be reported immediately a **G Form** should be sent without delay to the Sirene Bureau of the issuing Member State.

7.7. **Deletion of alerts on discreet and specific check**

An alert shall be deleted upon:

- (a) the expiry of the alert; or
- (b) a decision to delete by the competent authority of the issuing Member State.

7.8. **Automatic Number Plate Recognition systems (ANPR)**

See Section 9.



**▼ M1****8. ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE  
(ARTICLE 38 OF THE SIS II DECISION)****8.1. Multiple alerts**

See general procedure in Section 2.2.

**8.2. Vehicle alerts****8.2.1. *Checking for multiple alerts on a vehicle***

The mandatory identity description elements for checking for multiple alerts on a vehicle include:

(a) the registration/number plate, and/or

(b) the vehicle identification number (VIN).

Both numbers may feature in SIS II.

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

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

The identity description elements used for establishing whether two vehicle entries are identical are detailed in Section 2.2.3.

The consultation procedures for checking multiple and incompatible alerts to be applied by the Sirene Bureaux for vehicles shall be the same as for persons. For general procedures see Section 2.2.

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

**8.2.2. *VIN-twins***

VIN-twin refers to a vehicle, entered in SIS II, of the same type with the same vehicle identification number (VIN) as an original manufactured vehicle (e.g. a tractor and a motorcycle with the same VIN do not fall into this category). The following specific procedure shall apply to avoid the negative consequences of a repeated seizure of the original manufactured vehicle with the same VIN:

(a) Where the possibility of a VIN-twin is established, the Sirene Bureau shall, as appropriate:

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

▼ **M1**

- (ii) check the circumstances of the case giving rise to an alert in SIS II;
- (iii) find out the history of both vehicles from their production;
- (iv) request a thorough check of the seized vehicle, in particular its VIN, to verify whether it is the original manufactured vehicle.

All Sirene Bureaux involved shall closely cooperate in taking such measures.

- (b) Where the existence of a VIN-twin is confirmed, the issuing Member State shall consider whether it is necessary to maintain the alert in SIS II. If the Member State decides to maintain the alert in SIS II the issuing Member State shall:

- (i) add a vehicle-related remark 'Suspicion of clone' <sup>(1)</sup> in the alert;
  - (ii) invite the owner of the original manufactured vehicle to, subject to his explicit consent and according to national law, provide the Sirene Bureau of the issuing Member State with all relevant information required to avoid the negative consequences of misidentification.
  - (iii) Send out an **M form** via its Sirene Bureau to all other Bureaux including, as appropriate, the marks or features describing the original manufactured vehicle and distinguishing it from the vehicle entered in SIS II. The **M form** shall indicate words to the effect of 'ORIGINAL MANUFACTURED VEHICLE' prominently in field 083.
- (c) If, when SIS II is consulted, the vehicle-related remark, 'Suspicion of clone' is found, the user conducting the check shall contact the national Sirene Bureau to obtain additional information in order to clarify whether the vehicle being checked is the vehicle sought or the original manufactured vehicle.
  - (d) If during the check, it is established that the information on the **M form** is no longer up-to-date the Sirene Bureau of the executing Member State shall contact the Sirene Bureau of the issuing Member State in order to verify the current legal ownership of the vehicle. The latter Sirene Bureau shall send a new **M form** accordingly, indicating words to the effect of 'ORIGINAL MANUFACTURED VEHICLE' prominently in field 083.

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

The Sirene Bureaux may transmit further information on alerts entered under Article 38 of the SIS II Decision and in so doing may act on behalf of judicial authorities, if this information falls within the scope of mutual judicial assistance in accordance with national law.

<sup>(1)</sup> 'suspicion of clone' relates to cases where, for example, the registration documents of a vehicle are stolen and used to re-register another vehicle of the same make, model and colour which has also been stolen.

▼ **M1**

The Sirene Bureaux shall send supplementary information as quickly as possible via a **P form**, if requested in field 089 of a **G form**, when a hit is achieved on an alert for seizure or use as evidence issued on a vehicle, aircraft, boat, industrial equipment or container pursuant to Article 38 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.

Where a hit is achieved on an identifiable component of an object the Sirene Bureau of the executing Member State shall inform the Sirene Bureau of the issuing Member State of the circumstances of the hit using a **G form**, explaining in field 090 (Additional information) that the seizure is not of the complete object but of a component or components. Where several components are found at the same time, as they relate to one alert, only one **G form** will be sent. Any subsequent hits on the alert shall be notified to the Sirene Bureau of the issuing Member State by means of a **G form**. The alert shall not be deleted unless the conditions set out in Section 8.4 are met.

#### 8.4. **Deletion of alerts on objects for seizure or use as evidence in criminal proceedings**

An alert shall be deleted upon:

- (a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between Sirene Bureaux or the object becomes subject of another judicial or administrative procedure (e.g. judicial procedure on good faith purchase, disputed ownership or judicial cooperation on evidence);
- (b) the expiry of the alert; or
- (c) the decision to delete by the competent authority of the issuing Member State.

#### 9. **AUTOMATIC NUMBER PLATE RECOGNITION SYSTEMS (ANPR)**

These systems are relevant for alerts under Articles 36 and 38 of the SIS II Decision. Due to the widespread use of ANPR for law enforcement purposes there is the technical capability to achieve numerous hits on a vehicle or number plate over a short period of time.

Given that some ANPR sites are manned there is the possibility of a vehicle being detected and the requested action undertaken. In this case, before any action is undertaken, the users of the ANPR system shall verify whether the hit achieved through ANPR relates to an alert under Article 36 or 38 of the SIS II Decision.

However, many fixed ANPR sites are not constantly manned. Accordingly, although the technology will register the passage of the vehicle and a hit will be achieved, the requested action may not be undertaken.

▼ **M1**

For both Article 36 and Article 38 alerts where the requested action could not be taken the following general procedure shall apply:

One **H form** shall be sent for the first hit. If more information is required on the movement of the vehicle it is for the Sirene Bureau of the issuing Member State to contact the Sirene Bureau of the executing Member State bilaterally to discuss information needs.

For alerts under Article 36 the following procedure shall apply:

- (a) the Sirene Bureau of the Member State achieving the hit shall inform the issuing Sirene Bureau of the circumstances of the hit using one **G form**, using the word 'ANPR' in field 086. If more information is required on the movement of the vehicle, the Sirene Bureau of the issuing Member State shall contact the Sirene Bureau of the executing Member State;
- (b) the Sirene Bureau of the Member State achieving a hit on an alert for a **specific check** whereby the requested action could not be taken, shall inform the issuing Sirene bureau of the circumstances of the hit using an **H form**, with the word 'ANPR' in field 083, followed by words to the effect of: 'This hit has been achieved by use of ANPR. Please inform us if your country wishes to be informed of further hits achieved through ANPR for this vehicle or number plate where the requested action could not be undertaken';
- (c) the issuing Member State shall decide whether the alert has achieved its purpose, shall be deleted or not and whether bilateral discussions should take place on information needs.

For alerts under Article 38 the following procedure shall apply:

- (a) in circumstances where a hit occurs and the requested action has been taken the Sirene Bureau of the Member State achieving the hit shall inform the issuing Sirene Bureau of the circumstances of the hit using one **G form**;
- (b) in circumstances where a hit occurs and the requested action has not been taken the Sirene Bureau of the Member State achieving the hit shall inform the Sirene Bureau of the issuing Member State of the circumstances of the hit using an **H form** and the word 'ANPR' in field 083 followed by words to the effect of; 'This hit has been achieved by the use of ANPR. Please inform us if your country wishes to be informed of further hits achieved through ANPR for this vehicle or number plate where the requested action could not be taken.';

**▼ M1**

- (c) when receiving such an **H form**, the Sirene Bureau of the issuing Member State shall consult the competent authorities, which shall have the responsibility of deciding on the necessity of receiving further **H forms** or information passed bilaterally from the Sirene Bureau of the executing Member State.

**10. STATISTICS**

Once a year the Sirene Bureaux shall provide statistics, which have to be sent to the Agency 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.

Appendix 5 sets out the procedures and formats for the provision of statistics under this section.