III

(Acts adopted under the EU Treaty)

ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY

COUNCIL DECISION 2007/533/JHA

of 12 June 2007

on the establishment, operation and use of the second generation Schengen Information System (SIS II)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 30(1)(a) and (b), 31(1)(a) and (b) and 34(2)(c) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Whereas:

(1) The Schengen information system (SIS) set up pursuant to the provisions of Title IV of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2] (the Schengen Convention), and its development, SIS 1+, constitute an essential tool for the application of the provisions of the Schengen *acquis* as integrated into the framework of the European Union.

(2) The development of the second generation of SIS (SIS II) has been entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001 [3] and Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II) [4]. SIS II will replace SIS as created pursuant to the Schengen Convention.

(3) This Decision constitutes the necessary legislative basis for governing SIS II in respect of matters falling within the scope of the Treaty on European Union (the EU Treaty). 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) [5] constitutes the necessary legislative basis for governing SIS II in respect of matters falling within the scope of the Treaty establishing the European Community (the EC Treaty).

(4) The fact that the legislative basis necessary for governing SIS II consists of separate instruments does not affect the principle that SIS II constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical.

(5) SIS II should constitute a compensatory measure contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between police authorities and judicial authorities in criminal matters.

[1] Opinion of 25 October 2006 (not yet published in the Official Journal).

[2] OJ L 239, 22.9.2000, p. 19. Convention as amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).

[3] OJ L 328, 13.12.2001, p. 4.

[4] OJ L 328, 13.12.2001, p. 1.

[5] OJ L 381, 28.12.2006, p. 4.

(6) It is necessary to specify the objectives of SIS II, its technical architecture and financing, to lay down rules concerning its operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, the authorities authorised to access the data, the interlinking of alerts and further rules on data processing and the protection of personal data.

(7) SIS II is to include a central system (Central SIS II) and national applications. The expenditure involved in the operation of Central SIS II and related communication infrastructure should be charged to the general budget of the European Union.

(8) It is necessary to establish a manual setting out the detailed rules for the exchange of certain supplementary information concerning the action called for by alerts. National authorities in each Member State should ensure the exchange of this information.

(9) For a transitional period, the Commission should be responsible for the operational management of Central SIS II and of parts of the communication infrastructure. However, in order to ensure a smooth transition to SIS II, it may delegate some or all of these responsibilities to two national public sector bodies. In the long term, and following an impact assessment, containing a substantive analysis of alternatives from financial, operational and organisational perspective, and legislative proposals from the Commission, a management authority with responsibility for these tasks should be established. The transitional period should last for no more than five years from the date from which this Decision applies.

(10) SIS II is to contain alerts on persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes. In addition to alerts, it is appropriate to provide for the exchange of supplementary information which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States [1] should be processed in SIS II.

(11) It should be possible to add to SIS II a translation of the additional data entered for the purpose of surrender under the European Arrest Warrant and for the purpose of extradition.

(12) SIS II should contain alerts on missing persons to ensure their protection or to prevent threats, on persons wanted for judicial procedure, on persons and objects for discreet checks or specific checks and on objects for seizure or use as evidence in criminal proceedings.

(13) Alerts should not be kept in SIS II longer than the time required to fulfil the purposes for which they were supplied. As a general principle, alerts on persons should be automatically erased from SIS II after a period of three years. Alerts on objects entered for discreet checks or specific checks should be automatically erased from the SIS II after a period of five years. Alerts on objects for seizure or use as evidence in criminal proceedings should be automatically erased from SIS II after a period of 10 years. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the defined period and keep statistics about the number of alerts on persons the retention period of which has been extended.

(14) SIS II should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS II should also allow for the processing of data concerning individuals whose identity has been misused in order to avoid inconveniences caused by their misidentification, subject to suitable safeguards, in particular the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed.

(15) It should be possible for a Member State to add an indication, called a flag, to an alert, to the effect that the action to be taken on the basis of the alert will not be taken on its territory. When alerts are issued for arrest for surrender purposes, nothing in this Decision should be construed so as to derogate from or prevent the application of the provisions contained in the Framework Decision 2002/584/JHA. The decision to add a flag to an alert should be based only on the grounds for refusal contained in that Framework Decision.

(16) When a flag has been added and the whereabouts of the person wanted for arrest for surrender becomes known, the whereabouts should always be communicated to the issuing judicial authority, which may decide to transmit a European Arrest Warrant to the competent judicial authority in accordance with the provisions of the Framework Decision 2002/584/JHA.

(17) It should be possible for Member States to establish links between alerts in SIS II. The establishment by a Member State of links between two or more alerts should have no impact on the action to be taken, their retention period or the access rights to the alerts.

[1] OJ L 190, 18.7.2002, p. 1.

(18) Data processed in SIS II in application of this Decision should not be transferred or made available to third countries or to international organisations. However, it is appropriate to strengthen cooperation between the European Union and Interpol by promoting an efficient exchange of passport data. Where personal data is transferred from SIS II to Interpol, these personal data should be subject to an adequate level of protection, guaranteed by an agreement, providing strict safeguards and conditions.

(19) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The Convention allows exceptions and restrictions to the rights and obligations it provides, within certain limits. The personal data processed in the context of the implementation of this Decision should be protected in accordance with the principles of the Convention. The principles set out in the Convention should be supplemented or clarified in this Decision where necessary.

(20) The principles contained in Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 regulating the use of personal data in the police sector should be taken into account when personal data is processed by police authorities in application of this Decision.

(21) The Commission has submitted a proposal to the Council for a Framework Decision on the data protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which should be approved by the end of 2006 and be applied to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to this Decision.

(22) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [1] and in particular thereof concerning confidentiality and security of processing apply to the processing of personal data by the Community institutions and bodies when carrying out their responsibilities in the operational management of SIS II in the exercise of activities all or part of which fall within the scope of Community law. Part of the processing of personal data in SIS II falls within the scope of Community law. Consistent and homogeneous application of the rules regarding the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data requires clarification that, when the Commission is processing personal data in application of this Decision, Regulation (EC) No 45/2001 is applicable to it. The principles set out in Regulation (EC) No 45/2001 should be supplemented or clarified in this Decision where necessary.

(23) In so far as confidentiality is concerned, the relevant provisions of the Staff Regulations of Officials of the European Communities and the conditions of employment of other servants of the European Communities should apply to officials or other servants employed and working in connection with SIS II.

(24) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, appointed pursuant to Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty [2], should monitor the activities of the Community institutions and bodies in relation to the processing of personal data in view of the limited tasks of the Community institutions and bodies with regard to the data themselves.

(25) Both the Member States and the Commission should draw up a security plan in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues from a common perspective.

(26) The provisions of the Convention of 26 July 1995 on the establishment of a European Police Office [3] (hereinafter referred to as the 'Europol Convention') concerning data protection apply to the processing of SIS II data by Europol, including the powers of the Joint Supervisory Body, set up under the Europol Convention, to monitor the activities of Europol and liability for any unlawful processing of personal data by Europol.

(27) The provisions of Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime [4] concerning data protection apply to the processing of SIS II data by Eurojust, including the powers of the Joint Supervisory Body, set up under that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust.

[1] OJ L 8, 12.1.2001, p. 1.

[2] OJ L 12, 17.1.2004, p. 47.

[3] OJ C 316, 27.11.1995, p. 2.

[4] OJ L 63, 6.3.2002, p. 1.

(28) In order to ensure transparency, a report on the technical functioning of Central SIS II and the communication infrastructure, including its security, and on the exchange of supplementary information should be produced every two years by the Commission or, when it is established, the management authority. An overall evaluation should be issued by the Commission every four years.

(29) Certain aspects of SIS II such as technical rules on entering data, including data required for entering an alert, updating, deleting and searching data, rules on compatibility and priority of alerts, the adding of flags, links between alerts and exchange of supplementary information cannot owing to their technical nature, level of detail and need for regular updating be covered exhaustively by the provisions of this Decision. Implementing powers in respect of those aspects should therefore be delegated to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications. Subject to an impact assessment by the Commission, it should be decided to what extent the implementing measures could be the responsibility of the management authority, once it is set up.

(30) This Decision should define the procedure for the adoption of the measures necessary for its implementation. The procedure for adopting implementing measures under this Decision and Regulation (EC) No 1987/2006 should be the same.

(31) It is appropriate to lay down transitional provisions in respect of alerts issued in SIS 1+ which are to be transferred to SIS II. Some provisions of the Schengen *acquis* should continue to apply for a limited period of time until the Member States have examined the compatibility of those alerts with the new legal framework. The compatibility of alerts on persons should be examined as a matter of priority. Furthermore, any modification, addition, correction or update of an alert transferred from SIS 1+ to SIS II, as well as any hit on such an alert, should trigger an immediate examination of its compatibility with the provisions of this Decision.

(32) It is necessary to lay down special provisions regarding the part of the budget earmarked for the operations of SIS which is not part of the general budget of the European Union.

(33) Since the objectives of the action to be taken, namely the establishment and regulation of a joint information system, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the EC Treaty and referred to in Article 2 of the EU Treaty. In accordance with the principle of proportionality, as set out in Article 5 of the EC Treaty, this Decision does not go beyond what is necessary to achieve those objectives.

(34) This Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(35) The United Kingdom is taking part in this Decision, in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8(2) of Council Decision 2000/365/EC of 29 May 2000, concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* [1].

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

(37) This Decision is without prejudice to the arrangements for the United Kingdom and Ireland's partial participation in the Schengen *acquis*, as defined in Decisions 2000/365/EC and 2002/192/EC, respectively.

(38) As regards Iceland and Norway, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* [3], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC [4] on certain arrangements for the application of that Agreement.

(39) An arrangement should be made to allow representatives of Iceland and Norway to be associated with the work of committees assisting the Commission in the exercise of its implementing powers. Such an arrangement has been contemplated in the Exchanges of Letters between the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning committees which assist the European Commission in the exercise of its executive powers [5], annexed to the abovementioned Agreement.

---

[1] OJ L 131, 1.6.2000, p. 43.
[2] OJ L 64, 7.3.2002, p. 20.
[3] OJ L 176, 10.7.1999, p. 36.
[4] OJ L 176, 10.7.1999, p. 31.
[5] OJ L 176, 10.7.1999, p. 53.

(40) As regards Switzerland, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 4(1) of Council Decisions 2004/849/EC [1] and 2004/860/EC [2].

(41) An arrangement should be made to allow representatives of Switzerland to be associated with the work of committees assisting the Commission in the exercise of its implementing powers. Such an arrangement has been contemplated in the Exchange of Letters between the Community and Switzerland, annexed to the abovementioned Agreement.

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

(43) This Decision should apply to the United Kingdom, Ireland and Switzerland on dates determined in accordance with the procedures set out in the relevant instruments concerning the application of the Schengen *acquis* to those States,

HAS DECIDED AS FOLLOWS:

CHAPTER I

GENERAL PROVISIONS

Article 1

Establishment and general purpose of SIS II

1. A second generation Schengen Information System (SIS II) is hereby established.

2. The purpose of SIS II shall be, in accordance with this Decision, to ensure a high level of security within the 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 relating to the movement of persons in their territories, using information communicated via this system.

Article 2

Scope

1. This Decision establishes the conditions and procedures for the entry and processing in SIS II of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.

2. This Decision also lays down provisions on the technical architecture of SIS II, the responsibilities of the Member States and of the management authority referred to in Article 15, general data processing, the rights of the persons concerned and liability.

Article 3

Definitions

1. For the purposes of this Decision, the following definitions shall apply:

(a) 'alert' means a set of data entered in SIS II allowing the competent authorities to identify a person or an object with a view to taking specific action;

(b) 'supplementary information' means information not stored in SIS II, but connected to SIS II alerts, which is to be exchanged:

(i) in order to allow Member States to consult or inform each other when entering an alert;

(ii) following a hit in order to allow the appropriate action to be taken;

(iii) when the required action cannot be taken;

(iv) when dealing with the quality of SIS II data;

(v) when dealing with the compatibility and priority of alerts;

(vi) when dealing with rights of access;

(c) 'additional data' means the data stored in SIS II and connected with SIS II alerts which are to be immediately available to the competent authorities where a person in respect of whom data has been entered in SIS II is located as a result of searches made therein;

[1] Council Decision 2004/849/EC of 25 October 2004 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 368, 15.12.2004, p. 26).

[2] Council Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 370, 17.12.2004, p. 78).

(d) 'personal data' means any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly;

(e) 'processing of personal data' (processing) means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2. Any reference in this Decision to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Articles 24 and 38 of the EU Treaty for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via the Schengen Information System.

Article 4

Technical architecture and ways of operating the SIS II

1. SIS II shall be composed of:

(a) a central system (Central SIS II) composed of:

— a technical support function ('CS-SIS') containing a database, the 'SIS II database',

— a uniform national interface (NI-SIS);

(b) a national system (N.SIS II) in each of the Member States, consisting of the national data systems which communicate with 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;

(c) a communication infrastructure between CS-SIS and NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux as referred to in Article 7(2).

2. SIS II data shall be entered, updated, deleted and searched via the various N.SIS II systems. A national copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. It shall not be possible to search the data files of other Member States' N.SIS II.

3. CS-SIS, which performs technical supervision and administration functions, shall be located in Strasbourg (France) and a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system, shall be located in Sankt Johann im Pongau (Austria).

4. CS-SIS shall provide the services necessary for the entry and processing of SIS II data, including searches in the SIS II database. For the Member States which use a national copy CS-SIS shall:

(a) provide on-line update of the national copies;

(b) ensure synchronisation of and consistency between the national copies and the SIS II database;

(c) provide the operation for initialisation and restoration of the national copies.

Article 5

Costs

1. The costs of setting up, operating and maintaining Central SIS II and the Communication Infrastructure shall be borne by the general budget of the European Union.

2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).

3. The costs of setting up, operating and maintaining each N.SIS II shall be borne by the Member State concerned.

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 6

National systems

Each Member State shall be responsible for setting up, operating and maintaining its N.SIS II and connecting its N.SIS II to NI-SIS.

Article 7

N.SIS II Office and SIRENE Bureau

1. Each Member State shall designate an authority (the N.SIS II Office), which shall have central responsibility for its N.SIS II.

That authority shall be responsible for the smooth operation and security of the N.SIS II, shall ensure the access of the competent authorities to the SIS II and shall take the necessary measures to ensure compliance with the provisions of this Decision.

Each Member State shall transmit its alerts via its N.SIS II Office.

2. Each Member State shall designate the authority which shall ensure the exchange of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.

Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS II. For those purposes they shall have access to data processed in the SIS II.

3. The Member States shall inform the management authority of their N.SIS II office and of their SIRENE Bureau. The management authority shall publish the list of them together with the list referred to in Article 46(8).

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Should the Communication Infrastructure be unavailable, Member States may use other adequately secured technical means for exchanging supplementary information.

2. Supplementary information shall be used only for the purpose for which it was transmitted.

3. Requests for supplementary information made by other Member States shall be answered as soon as possible.

4. Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 67 in the form of a manual called the 'SIRENE Manual', without prejudice to the provisions of the instrument setting up the management authority.

Article 9

Technical compliance

1. To ensure the prompt and effective transmission of data, each Member State shall observe, when setting up its N.SIS II, the protocols and technical procedures established to ensure the compatibility of its N-SIS II with CS-SIS. These protocols and technical procedures shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the management authority.

2. If a Member State uses a national copy it shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy are, by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS II database, and that a search in its national copy produces a result equivalent to that of a search in the SIS II database.

Article 10

Security – Member States

1. Each Member State shall, in relation to its N.SIS II, adopt the necessary measures, including a security plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);

(g) ensure that all authorities with a right of access to SIS II or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 60 without delay upon their request (personnel profiles)

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control);

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Decision (self-auditing).

2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the exchange of supplementary information.

Article 11

Confidentiality – Member States

Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS II data and supplementary information, in accordance with its national legislation. This obligation shall also apply after those people leave office or employment or after the termination of the activities of those bodies.

Article 12

Keeping of records at national level

1. Member States not using national copies shall ensure that every access to and all exchanges of personal data within CS-SIS are recorded in their N.SIS II for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS II, data integrity and security.

2. Member States using national copies shall ensure that every access to and all exchanges of SIS II data are recorded for the purposes specified in paragraph 1. This does not apply to the processes referred to in Article 4(4).

3. The records shall show, in particular, the history of the alerts, the date and time of the data transmission, the data used to perform a search, a reference to the data transmitted and the name of both the competent authority and the person responsible for processing the data.

4. The records may be used only for the purpose mentioned in paragraph 1 and 2 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The records which include the history of alerts shall be erased one to three years after deletion of the alerts.

5. Records may be kept longer if they are required for monitoring procedures that are already under way.

6. The competent national authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS II, data integrity and security, shall have access, within the limits of their competence and at their request, to these records for the purpose of fulfilling their duties.

Article 13

Self-monitoring

Member States shall ensure that each authority entitled to access SIS II data takes the measures necessary to comply with this Decision and cooperates, where necessary, with the national supervisory authority.

Article 14

Staff training

Before being authorised to process data stored in SIS II, the staff of the authorities having a right to access SIS II shall receive appropriate training about data-security and data-protection rules and shall be informed of any relevant criminal offences and penalties.

CHAPTER III

RESPONSIBILITIES OF THE MANAGEMENT AUTHORITY

Article 15

Operational management

1. After a transitional period, a management authority (the Management Authority), funded by the general budget of the European Union, shall be responsible for the operational management of Central SIS II. The Management Authority shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for Central SIS II.

2. The Management Authority shall also be responsible for the following tasks relating to the Communication Infrastructure:

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider.

3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:

(a) tasks relating to implementation of the budget;

(b) *acqui*sition and renewal;

(c) contractual matters.

4. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of Central SIS II. The Commission may delegate that task and tasks relating to implementation of the budget in accordance with the Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities [1], to national public-sector bodies, in two different countries.

5. Each national public sector body, as referred to in paragraph 4, must comply in particular with the following selection criteria:

(a) it must demonstrate that it has a lengthy experience in operating a large-scale information system with the functionalities referred to in Article 4(4);

(b) it must have considerable expertise in the service and security requirements of an information system with functionalities comparable to those referred to in Article 4(4);

(c) it must have sufficient and experienced staff with the appropriate professional expertise and linguistic skills to work in an international cooperation environment such as that required by SIS II;

(d) it must have a secure and custom-built facility infrastructure available, in particular, to backup and guarantee the continuous functioning of large-scale IT systems; and

(e) its administrative environment must allow it to implement its tasks properly and avoid any conflict of interests.

6. Prior to any such delegation as referred to in paragraph 4 and at regular intervals thereafter, the Commission shall inform the European Parliament and the Council of the terms of the delegation, its precise scope, and the bodies to which tasks are delegated.

7. Where the Commission delegates its responsibility during the transitional period pursuant to paragraph 4, it shall ensure that this delegation fully respects the limits set by the institutional system laid out in the EC Treaty. It shall ensure, in particular, that this delegation does not adversely affect any effective control mechanism under European Union law, whether of the Court of Justice, the Court of Auditors or the European Data Protection Supervisor.

8. Operational management of Central SIS II shall consist of all the tasks necessary to keep Central SIS II functioning 24 hours a day, seven days a week in accordance with this Decision, in particular the maintenance work and technical developments necessary for the smooth running of the system.

[1] OJ L 248, 16.9.2002, p. 1.

Article 16

Security

1. The Management Authority, in relation to Central SIS II and the Commission in relation to the Communication Infrastructure, shall adopt the necessary measures, including of a security plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation by means of individual and unique user identities and confidential access modes only (data access control);

(g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 61 without delay upon its request (personnel profiles);

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom the data were input (input control);

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control);

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Decision (self-auditing).

2. The Management Authority shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the exchange of supplementary information through the Communication Infrastructure.

Article 17

Confidentiality – Management Authority

1. Without prejudice to Article 17 of the Staff Regulations of officials of the European Communities, the Management Authority shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those provided in Article 11 in this Decision to all its staff required to work with SIS II data. This obligation shall also apply after those people leave office or employment or after the termination of their activities.

2. The Management Authority shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the communication infrastructure.

Article 18

Keeping of records at central level

1. The Management Authority shall ensure that every access to and all exchanges of personal data within CS-SIS are recorded for the purposes mentioned in Article 12(1) and (2).

2. The records shall show, in particular, the history of the alerts, the date and time of the data transmitted, the data used to perform searches, the reference to the data transmitted and the name of the competent authority responsible for processing the data.

3. The records may only be used for the purposes mentioned in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The records which include the history of alerts shall be erased after one to three years after deletion of the alerts.

4. Records may be kept longer if they are required for monitoring procedures that are already underway.

5. The competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to those records for the purpose of fulfilling their tasks.

Article 19

Information campaign

The Commission shall, in cooperation with the national supervisory authorities, and the European Data Protection Supervisor accompany the start of the operation of SIS II with an information campaign informing the public about the objectives, the data stored, the authorities having access and the rights of persons. After its establishment, the Management Authority, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall repeat such campaigns regularly. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens about SIS II generally.

CHAPTER IV

CATEGORIES OF DATA AND FLAGGING

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Decision providing for the storage of additional data, SIS II shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 26, 32, 34, 36 and 38.

2. The categories of data shall be as follows:

(a) persons in relation to whom an alert has been issued;

(b) objects referred to in Articles 36 and 38.

3. The information on persons in relation to whom an alert has been issued shall be no more than the following:

(a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately;

(b) any specific, objective, physical characteristics not subject to change;

(c) place and date of birth;

(d) sex;

(e) photographs;

(f) fingerprints;

(g) nationality(ies);

(h) whether the person concerned is armed, violent or has escaped;

(i) reason for the alert;

(j) authority issuing the alert;

(k) a reference to the decision giving rise to the alert;

(l) action to be taken;

(m) link(s) to other alerts issued in SIS II pursuant to Article 52;

(n) the type of offence.

4. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority.

5. The technical rules necessary for searching data referred to in paragraph 3 shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 46(2).

Article 21

Proportionality

Before issuing an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II.

Article 22

Specific rules for photographs and fingerprints

The use of photographs and fingerprints as referred to in Article 20(3)(e) and (f) shall be used subject to the following provisions:

(a) photographs and fingerprints shall only be entered following a special quality check to ascertain the fulfilment of a minimum data quality standard. The specification of the special quality check shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority;

(b) photographs and fingerprints 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.

(c) as soon as this becomes technically possible, fingerprints may also be used to identify a person on the basis of his biometric identifier. Before this functionality is implemented in SIS II, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted.

Article 23

Requirement for an alert to be entered

1. Alerts on persons may not be entered without the data referred to in Article 20(3)(a), (d), (l) as well as, where applicable, (k).

2. When available, all other data listed in Article 20(3) shall also be entered.

Article 24

General provisions on flagging

1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 or 36 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 Member State which entered the alert.

2. 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.

3. 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.

Article 25

Flagging related to alerts for arrest for surrender purposes

1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall only be added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.

2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused.

CHAPTER V

ALERTS IN RESPECT OF PERSONS WANTED FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES

Article 26

Objectives and conditions for issuing alerts

1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the issuing Member State.

2. Data on persons wanted for arrest for surrender purposes shall also be entered on the basis of arrest warrants issued in accordance with Agreements concluded between the European Union and third countries on the basis of Articles 24 and 38 of the EU Treaty for the purpose of surrender of persons on the basis of an arrest warrant, which provide for the transmission of such an arrest warrant via the Schengen Information System.

Article 27

Additional data on persons wanted for arrest for surrender purposes

1. If a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant the issuing Member State shall enter in SIS II a copy of the original of the European Arrest Warrant.

2. The issuing Member State may enter a copy of a translation of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.

Article 28

Supplementary information on persons wanted for arrest for surrender purposes

The Member State which entered the alert in SIS II for arrest for surrender purposes shall communicate the information referred to in Article 8(1) of Framework Decision 2002/584/JHA to all Member States through the exchange of supplementary information.

Article 29

Supplementary information on persons wanted for arrest for extradition purposes

1. The Member State which entered the alert into SIS II for extradition purposes shall communicate the following data to all Member States through the exchange of supplementary information to all Member States:

(a) the authority which issued the request for arrest;

(b) whether there is an arrest warrant or a document having the same legal effect, or an enforceable judgment;

(c) the nature and legal classification of the offence;

(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;

(e) in so far as possible, the consequences of the offence;

(f) any other information useful or necessary for the execution of the alert.

2. The data mentioned in paragraph 1 shall not be communicated where the data referred to in Articles 27 or 28 have already been provided and are considered sufficient for the execution of the alert by the Member State concerned.

Article 30

Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes

If an arrest cannot be made, either because a requested Member State refuses in accordance with the procedures on flagging set out in Articles 24 or 25, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, the requested Member State must regard the alert as being an alert for the purposes of communicating the whereabouts of the person concerned.

Article 31

Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition

1. An alert entered in SIS II in accordance with Article 26 in conjunction with the additional data referred to in Article 27, shall constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies.

2. Where Framework Decision 2002/584/JHA does not apply, an alert entered in SIS II in accordance with Articles 26 and 29 shall have the same legal force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 December 1957 or Article 15 of the Benelux Treaty concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962.

CHAPTER VI

ALERTS ON MISSING PERSONS

Article 32

Objectives and conditions for issuing alerts

1. Data on missing persons who need to be placed under protection and/or whose whereabouts need to be ascertained shall be entered in SIS II at the request of the competent authority of the Member State issuing the alert.

2. The following categories of missing persons may be entered:

(a) missing persons who need to be placed under protection

  (i) for their own protection;

  (ii) in order to prevent threats;

(b) missing persons who do not need to be placed under protection.

3. Paragraph 2(a) shall apply only to persons who must be interned following a decision by a competent authority.

4. Paragraphs 1, 2 and 3 shall apply in particular to minors.

5. Member States shall ensure that the data entered in SIS II indicate which of the categories mentioned in paragraph 2 the missing person falls into.

Article 33

Execution of action based on an alert

1. Where a person as referred to in Article 32 is located, the competent authorities shall, subject to paragraph 2, communicate his whereabouts to the Member State issuing the alert. They may, in the cases referred to in Article 32(2)(a) move the person to a safe place in order to prevent him from continuing his journey, if so authorised by national law.

2. The communication, other than between the competent authorities, of data on a missing person who has been located and who is of age shall be subject to that person's consent. However, the competent authorities may communicate the fact that the alert has been erased because the person has been located to the person who reported the person missing.

CHAPTER VII

ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE

Article 34

Objectives and conditions for issuing alerts

For the purposes of communicating their place of residence or domicile Member States shall, at the request of a competent authority, enter in SIS II data on:

(a) witnesses;

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

(c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted;

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

Article 35

Execution of the action based on an alert

Requested information shall be communicated to the requesting Member State through the exchange of supplementary information.

CHAPTER VIII

ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS OR SPECIFIC CHECKS

Article 36

Objectives and conditions for issuing alerts

1. Data on persons or vehicles, boats, aircrafts and containers shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks or specific checks in accordance with Article 37(4).

2. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:

(a) where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or

(b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA.

3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted.

4. Alerts on vehicles, boats, aircrafts and containers may be issued where there is a clear indication that they are connected with the serious criminal offences referred to in paragraph 2 or the serious threats referred to in paragraph 3.

Article 37

Execution of the action based on an alert

1. For the purposes of discreet checks or specific checks, all or some of the following information shall be collected and communicated to the authority issuing the alert when border control or other police and customs checks are carried out within a Member State:

(a) the fact that the person for whom, or the vehicle, boat, aircraft or container, for which an alert has been issued, has been located;

(b) the place, time or reason for the check;

(c) the route and destination of the journey;

(d) the persons accompanying the persons concerned or the occupants of the vehicle, boat or aircraft who can reasonably be expected to be associated to the persons concerned;

(e) the vehicle, boat, aircraft or container used;

(f) objects carried;

(g) the circumstances under which the person or the vehicle, boat, aircraft or container was located.

2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.

3. For the collection of the information referred to in paragraph 1, Member States shall take the necessary steps not to jeopardise the discreet nature of the check.

4. During specific checks, persons, vehicles, boats, aircraft, containers and objects carried, may be searched in accordance with national law for the purposes referred to in Article 36. If specific checks are not authorised under the law of a Member State, they shall automatically be replaced, in that Member State, by discreet checks.

CHAPTER IX

ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS

Article 38

Objectives and conditions for issuing alerts

1. Data on objects sought for the purposes of seizure or use as evidence in criminal proceedings shall be entered in SIS II.

2. The following categories of readily identifiable objects shall be entered:

(a) motor vehicles with a cylinder capacity exceeding 50cc, boats and aircrafts;

(b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers;

(c) firearms;

(d) blank official documents which have been stolen, misappropriated or lost;

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

(f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated;

(g) banknotes (registered notes);

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

3. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority.

Article 39

Execution of the action based on an alert

1. If a search brings to light an alert for an object which has been located, the authority which matched the two items of data shall contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Decision.

2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.

3. The Member State which located the object shall take measures in accordance with national law.

CHAPTER X

RIGHT TO ACCESS AND RETENTION OF ALERTS

Article 40

Authorities having a right to access alerts

1. Access to data entered in SIS II and the right to search such data directly or in a copy of SIS II data shall be reserved exclusively to the authorities responsible for:

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

(b) other police and customs checks carried out within the Member State concerned, the coordination of such checks by designated authorities.

2. However, the right to access data entered in SIS II and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.

[1] OJ L 105, 13.4.2006, p. 1.

3. The authorities referred to in this Article shall be included in the list referred to in Article 46(8).

Article 41

Access to SIS II data by Europol

1. The European Police Office (Europol) shall within its mandate have the right to access and search directly, data entered into SIS II in accordance with Articles 26, 36 and 38.

2. Where a search by Europol reveals the existence of an alert in SIS II, Europol shall inform, via the channels defined by the Europol Convention the Member State which issued the alert thereof.

3. Use of information obtained from a search in the SIS II is subject to the consent of the Member State concerned. If the Member State allows the use of such information, the handling thereof shall be governed by the Europol Convention. Europol may only communicate such information to third countries and third bodies with the consent of the Member State concerned.

4. Europol may request further information from the Member State concerned in accordance with the provisions of the Europol Convention.

5. Europol shall:

(a) record every access and search made by it, in accordance with the provisions of Article 12;

(b) without prejudice to paragraphs 3 and 4, not connect parts of SIS II nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS II;

(c) limit access to data entered in SIS II to specifically authorised staff of Europol;

(d) adopt and apply measures provided for in Articles 10 and 11;

(e) allow the Joint Supervisory Body, set up under Article 24 of the Europol Convention, to review the activities of Europol in the exercise of its right to access and search data entered in SIS II.

Article 42

Access to SIS II data by Eurojust

1. The national members of Eurojust and their assistants shall, within their mandate, have the right to access and search data entered in SIS II, in accordance with Articles 26, 32, 34 and 38.

2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS II, he shall inform the Member State having issued the alert thereof. Any communication of information obtained from such a search may only be communicated to third countries and third bodies with the consent of the Member State which issued the alert.

3. Nothing in this Article shall be interpreted as affecting the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.

4. Every access and search made by a national member of Eurojust or an assistant shall be recorded in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be registered.

5. No parts of SIS II shall be connected nor shall the data contained therein to which the national members or their assistants have access be transferred to any computer system for data collection and processing operated by or at Eurojust nor shall any part of SIS II be downloaded.

6. Access to data entered in SIS II shall be limited to the national members and their assistants and shall not be extended to Eurojust staff.

7. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied.

Article 43

Scope of access

Users, including Europol, the national members of Eurojust and their assistants, may only access data which they require for the performance of their tasks.

Article 44

Retention period of alerts on persons

1. Alerts on persons entered in SIS II pursuant to this Decision shall be kept only for the time required to achieve the purposes for which they were entered.

2. A Member State issuing an alert shall, within three years of its entry into SIS II, review the need to keep it. The period shall be one year in the case of alerts on persons pursuant to Article 36.

3. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

4. Within the review period, the Member State issuing the alert may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. In such a case paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.

5. Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the Member State issuing the alert has communicated the extension of the alert to CS-SIS pursuant to paragraph 4. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.

6. Member States shall keep statistics about the number of alerts the retention period of which has been extended in accordance with paragraph 4.

Article 45

Retention period of alerts on objects

1. Alerts on objects entered in SIS II pursuant to this Decision shall be kept only for the time required to achieve the purposes for which they were entered.

2. Alerts on objects entered in accordance with Article 36 shall be kept for a maximum of five years.

3. Alerts on objects entered in accordance with Article 38 shall be kept for a maximum of 10 years.

4. The retention periods referred to in paragraphs 2 and 3 may be extended should this prove necessary for the purposes for which the alert was issued. In such a case, paragraphs 2 and 3 shall apply also to the extension.

CHAPTER XI

GENERAL DATA PROCESSING RULES

Article 46

Processing of SIS II data

1. The Member States may process the data referred to in Articles 20, 26, 32, 34, 36 and 38 only for the purposes laid down for each category of alert referred to in those Articles.

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 40 to carry out a direct search. The provisions of this Decision shall apply to such copies. Alerts issued by one Member State may not be copied from its N.SIS II into other national data files.

3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end.

Member States shall keep an up-to-date inventory of such copies, make this inventory available to their national supervisory authority, and ensure that the provisions of this Decision, in particular those of Article 10, are applied in respect of such copies.

4. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 40 and to duly authorised staff.

5. With regard to the alerts laid down in Articles 26, 32, 34, 36 and 38 of this Decision, any processing of information contained therein for purposes other than those for which it was entered in SIS II must be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. Prior authorisation from the Member State issuing the alert must be obtained for this purpose.

6. Data may not be used for administrative purposes.

7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State.

8. Each Member State shall send to the Management Authority a list of its competent authorities which are authorised to search directly the data contained in SIS II pursuant to this Decision, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. The Management Authority shall ensure the annual publication of the list in the *Official Journal of the European Union*.

9. In so far as European Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS II.

Article 47

SIS II data and national files

1. Article 46(2) shall not prejudice the right of a Member State to keep in its national files SIS II data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.

2. Article 46(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS II by that Member State.

Article 48

Information in case of non-execution of alert

If a requested action cannot be performed, the requested Member State shall immediately inform the Member State issuing the alert.

Article 49

Quality of the data processed in SIS II

1. A Member State issuing an alert shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS II lawfully.

2. Only the Member State issuing an alert shall be authorised to modify, add to, correct, update or delete data which it has entered.

3. If a Member State other than that which issued an alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the Member State that issued the alert thereof at the earliest opportunity and not later than 10 days after the said evidence has come to its attention. The Member State that issued the alert shall check the communication and, if necessary, correct or delete the item in question without delay.

4. If the Member States are unable to reach agreement within two months, the Member State which did not issue the alert shall submit the matter to the European Data Protection Supervisor who shall, jointly with the national supervisory authorities concerned, act as mediator.

5. The Member States shall exchange supplementary information if a person complains that he is not the person wanted by an alert. If the outcome of the check is that there are in fact two different persons the complainant shall be informed of the provisions of Article 51.

6. Where a person is already the subject of an alert in SIS II, a Member State which enters a further alert shall reach agreement on the entry of the alert with the Member State which entered the first alert. The agreement shall be reached on the basis of the exchange of supplementary information.

Article 50

Distinguishing between persons with similar characteristics

Where it becomes apparent, when a new alert is entered, that there is already a person in SIS II with the same identity description element, the following procedure shall be followed:

(a) the SIRENE Bureau shall contact the requesting authority to clarify whether or not the alert is on the same person;

(b) if the cross-check reveals that the subject of the new alert and the person already in SIS II are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 49(6). If the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.

Article 51

Additional data for the purpose of dealing with misused identities

1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has been misused, the Member State which entered the alert shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification.

2. Data relating to a person whose identity has been misused shall be used only for the following purposes:

(a) to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert;

(b) to allow the person whose identity has been misused to prove his identity and to establish that his identity has been misused.

3. For the purpose of this Article, no more than the following personal data may be entered and further processed in SIS II:

(a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases possibly entered separately;

(b) any specific objective and physical characteristic not subject to change;

(c) place and date of birth;

(d) sex;

(e) photographs;

(f) fingerprints;

(g) nationality(ies);

(h) number(s) of identity paper(s) and date of issue.

4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority.

5. The data referred to in paragraph 3 shall be erased at the same time as the corresponding alert or earlier if the person so requests.

6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.

Article 52

Links between alerts

1. A Member State may create a link between alerts it enters in SIS II. The effect of such a link shall be to establish a relationship between two or more alerts.

2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention period of each of the linked alerts.

3. The creation of a link shall not affect the rights of access provided for in this Decision. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.

4. A Member State shall create a link between alerts only when there is a clear operational need.

5. Links may be created by a Member State in accordance with its national legislation provided that the principles outlined in the present Article are respected.

6. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.

7. The technical rules for linking alerts shall be adopted in accordance with the procedure defined in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority.

Article 53

Purpose and retention period of supplementary information

1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau to support the exchange of supplementary information.

2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS II.

3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.

Article 54

Transfer of personal data to third parties

Data processed in SIS II pursuant to this Decision shall not be transferred or made available to third countries or to international organisations.

Article 55

Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol

1. By way of derogation from Article 54, the passport number, country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered in SIS II may be exchanged with members of Interpol by establishing a connection between SIS II and the Interpol database on stolen or missing travel documents, subject to the conclusion of an Agreement between Interpol and the European Union. The Agreement shall provide that the transmission of data entered by a Member State shall be subject to the consent of that Member State.

2. The Agreement referred to in paragraph 1 shall foresee that the data shared shall only be accessible to members of Interpol from countries that ensure an adequate level of protection of personal data. Before concluding this Agreement, the Council shall seek the opinion of the Commission on the adequacy of the level of protection of personal data and respect of fundamental rights and liberties regarding the automatic processing of personal data by Interpol and by countries which have delegated members to Interpol.

3. The Agreement referred to in paragraph 1 may also provide for access through SIS II for the Member States to data from the Interpol database on stolen or missing travel documents, in accordance with the relevant provisions of this Decision governing alerts on stolen, misappropriated, lost and invalidated passports entered in SIS II.

CHAPTER XII

DATA PROTECTION

Article 56

Processing of sensitive categories of data

Processing of the categories of data listed in the first sentence of Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, shall be prohibited.

Article 57

Application of the Council of Europe Data Protection Convention

Personal data processed in application of this Decision shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, and subsequent amendments thereto.

Article 58

Right of access, correction of inaccurate data and deletion of unlawfully stored data

1. The right of persons to have access to data relating to them entered in SIS II in accordance with this Decision shall be exercised in accordance with the law of the Member State before which they invoke that right.

2. If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what procedures.

3. A Member State other than that which has issued an alert may communicate information concerning such data only if it first gives the Member State issuing the alert an opportunity to state its position. This shall be done through the exchange of supplementary information.

4. Information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties.

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

6. The individual concerned shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides.

7. The individual shall be informed about the follow-up given to the exercise of his rights of correction and deletion as soon as possible and in any event not later than three months from the date on which he applies for correction or deletion or sooner if national law so provides.

Article 59

Remedies

1. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him.

2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 64.

3. The rules on remedies provided for in this Article shall be evaluated by the Commission by 23 August 2009.

Article 60

Supervision of N.SIS II

1. Each Member State shall ensure that an independent authority (the national supervisory authority) monitors independently the lawfulness of the processing of SIS II personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information.

2. The national supervisory authority shall ensure that an audit of the data processing operations in its N.SIS II is carried out in accordance with international auditing standards at least every four years.

3. Member States shall ensure that their national supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Decision.

Article 61

Supervision of the Management Authority

1. The European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with this Decision. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.

2. The European Data Protection Supervisor shall ensure that an audit of the Management Authority's personal data processing activities is carried out in accordance with international auditing standards at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Management Authority, the Commission and the National Supervisory Authorities. The Management Authority shall be given an opportunity to make comments before the report is adopted.

Article 62

Cooperation between national supervisory authorities and the European Data Protection Supervisor

1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of SIS II.

2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Decision, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. The national supervisory authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years.

Article 63

Data protection during the transitional period

Where the Commission delegates its responsibilities during the transitional period to another body or bodies, pursuant to Article 15(4), it shall ensure that the European Data Protection Supervisor has the right and is able to fully exercise his tasks, including carrying out on-the-spot checks and to exercise any other powers conferred on him by Article 47 of Regulation (EC) No 45/2001.

CHAPTER XIII

LIABILITY AND PENALTIES

Article 64

Liability

1. Each Member State shall be liable in accordance with its national law for any damage caused to a person through the use of N.SIS II. This shall also apply to damage caused by the Member State which issued the alert, where the latter entered factually inaccurate data or stored data unlawfully.

2. If the Member State against which an action is brought is not the Member State issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the use of data by the Member State requesting reimbursement infringes this Decision.

3. If any failure by a Member State to comply with its obligations under this Decision causes damage to SIS II, that Member State shall be held liable for such damage, unless and in so far as the Management Authority or another Member States participating in SIS II failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

Article 65

Penalties

Member States shall ensure that any misuse of data entered in SIS II or any exchange of supplementary information contrary to this Decision is subject to effective, proportionate and dissuasive penalties in accordance with national law.

CHAPTER XIV

FINAL PROVISIONS

Article 66

Monitoring and statistics

1. The Management Authority shall ensure that procedures are in place to monitor the functioning of SIS II against objectives, relating to output, cost-effectiveness, security and quality of service.

2. For the purposes of technical maintenance, reporting and statistics, the Management Authority shall have access to the necessary information relating to the processing operations performed in Central SIS II.

3. Each year the Management Authority shall publish statistics showing the number of records per category of alert, the number of hits per category of alert and how many times SIS II was accessed, in total and for each Member State.

4. Two years after SIS II is brought into operation and every two years thereafter, the Management Authority shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS II and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.

5. Three years after SIS II is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS II and the bilateral and multilateral exchange of supplementary information between Member States. This overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Decision in respect of Central SIS II, the security of Central SIS II and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.

6. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 4 and 5.

7. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.

Article 67

Regulatory Committee

1. Where reference is made to this Article, the Commission shall be assisted by a regulatory Committee composed of the representatives of the Member States and chaired by the representative of the Commission. The representative of the Commission shall submit to the Committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the Chair may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the EC Treaty in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the Committee shall be weighted in the manner set out in that Article. The Chair shall not vote.

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the *Official Journal of the European Union*.

3. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall, without delay, submit to the Council a proposal relating to the measures to be taken.

4. The Council may act by qualified majority on the proposal, within a period of two months from the date of referral to the Council. If within that period the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, re-submit its proposal or present a legislative proposal. If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

5. The Committee referred to in paragraph 1 shall exercise its function from 23 August 2007.

Article 68

Amendment of the provisions of the Schengen *acquis*

1. For the purposes of matters falling within the scope of the EU Treaty, this Decision shall replace on the date referred to in Article 71(2) the provisions of Articles 64 and 92 to 119 of the Schengen Convention, with the exception of Article 102 A thereof.

2. For the purposes of matters falling within the scope of the EU Treaty, this Decision shall replace, on the date referred to in Article 71(2), the following provisions of the Schengen *acquis* implementing those Articles [1]:

(a) Decision of the Executive Committee of 14 December 1993 on the Financial Regulation on the costs of installing and operating the Schengen information system (C.SIS) (SCH/Com-ex (93) 16);

(b) Decision of the Executive Committee of 7 October 1997 on the development of the SIS (SCH/Com-ex (97) 24);

(c) Decision of the Executive Committee of 15 December 1997 amending the Financial Regulation on C.SIS (SCH/Com-ex (97) 35);

(d) Decision of the Executive Committee of 21 April 1998 on C.SIS with 15/18 connections (SCH/Com-ex (98) 11);

(e) Decision of the Executive Committee of 25 April 1997 on awarding the contract for the SIS II Preliminary Study (SCH/Com-ex (97) 2 rev. 2);

(f) Decision of the Executive Committee of 28 April 1999 on C.SIS installation expenditure (SCH/Com-ex (99) 4);

(g) Decision of the Executive Committee of 28 April 1999 on updating the SIRENE Manual (SCH/Com-ex (99) 5);

(h) Declaration of the Executive Committee of 18 April 1996 defining the concept of alien (SCH/Com-ex (96) decl. 5);

(i) Declaration of the Executive Committee of 28 April 1999 on the structure of SIS (SCH/Com-ex (99) decl. 2 rev.);

(j) Decision of the Executive Committee of 7 October 1997 on contributions from Norway and Iceland to the costs of installing and operating of the C.SIS (SCH/Com-ex (97) 18).

3. For the purposes of matters falling within the scope of the EU Treaty, references to the replaced Articles of the Schengen Convention and relevant provisions of the Schengen *acquis* implementing those Articles shall be construed as references to this Decision.

Article 69

Repeal

Decision 2004/201/JHA, Decision 2005/211/JHA, Decision 2005/719/JHA, Decision 2005/727/JHA, Decision 2006/228/JHA, Decision 2006/229/JHA, and Decision 2006/631/JHA are repealed on the date referred to in Article 71(2).

[1] OJ L 239, 22.9.2000, p. 439.

Article 70

Transitional period and budget

1. Alerts shall be transferred from SIS 1+ to SIS II. The Member States shall ensure, giving priority to alerts on persons, that the contents of the alerts that are transferred from SIS 1+ to SIS II satisfy the provisions of this Decision as soon as possible and within three years after the date referred to in Article 71(2) at the latest. During this transitional period, the Member States may continue to apply the provisions of Articles 94, 95, and 97-100 of the Schengen Convention to the contents of the alerts that are transferred from SIS 1+ to SIS II subject to the following rules:

(a) in the event of a modification of, an addition to or a correction or update of the content of an alert transferred from SIS 1+ to SIS II, the Member States shall ensure that the alert satisfies the provisions of this Decision as from the time of that modification, addition, correction or update;

(b) in the event of a hit on an alert transferred from SIS 1+ to SIS II, the Member States shall examine the compatibility of that alert with the provisions of this Decision immediately but without delaying the action to be taken on the basis of that alert.

2. The remainder of the budget at the date set in accordance with Article 71(2), which has been approved in accordance with the provisions of Article 119 of the Schengen Convention, shall be paid back to the Member States. The amounts to be repaid shall be calculated on the basis of the contributions from the Member States as laid down in the Decision of the Executive Committee of 14 December 1993 on the financial regulation on the costs of installing and operating the Schengen Information System.

3. During the transitional period referred to in Article 15(4), references in this Decision to the Management Authority shall be construed as references to the Commission.

Article 71

Entry into force, applicability and migration

1. This Decision shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

2. It shall apply to the Member States participating in SIS 1+ from dates to be fixed by the Council, acting by the unanimity of its Members representing the Governments of the Member States participating in SIS 1+.

3. The dates referred to in paragraph 2 shall be fixed after:

(a) the necessary implementing measures have been adopted;

(b) all Member States fully participating in SIS 1+ have notified the Commission that they have made the necessary technical and legal arrangements to process SIS II data and exchange supplementary information;

(c) the Commission has declared the successful completion of a comprehensive test of SIS II, which shall be conducted by the Commission together with the Member States, and the preparatory bodies of the Council have validated the proposed test result and confirmed that the level of performance of SIS II is at least equivalent to that achieved with SIS 1+;

(d) the Commission has made the necessary technical arrangements for allowing Central SIS II to be connected to N.SIS II of the Member States concerned.

4. The Commission shall inform the European Parliament of the results of the tests carried out in accordance with paragraph 3(c).

5. Any Decision of the Council taken in accordance with paragraph 2 shall be published in the *Official Journal of the European Union*.

Done at Luxembourg, 12 June 2007.

For the Council,
The President
W. SCHÄUBLE