P6_TA-PROV(2006)0445

Establishment, operation and use of SIS II (regulation) ***I

European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) (COM(2005)0236 – C6-0174/2005 – 2005/0106(COD))

(Codecision procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to the European Parliament and the Council (COM(2005)0236)[1],

– having regard to Article 251(2) and Articles 62(2)(a) and 66 of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0174/2005),

– having regard to Rule 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Budgets (A6-0355/2006),

1. Approves the Commission proposal as amended;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council and Commission.

[1] Not yet published in OJ.

PROPOSAL FOR A REGULATION

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment, operation and use of the second generation Schengen information system (SIS II)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles
62(2)(a), 63(3)(b) and Article 66 thereof,

Having regard to the proposal from the Commission[2],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[3],

Whereas :

(1) The Schengen information system (hereinafter referred to as "SIS 1+") 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[4] (hereinafter referred to as the "Schengen Convention"), constitutes 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 the SIS (hereinafter, referred to as "SIS II") has been entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[5] and Council Decision No 2001/886/JHA[6] of 6 December 2001 on the development of the second generation Schengen Information System (SIS II). The SIS II will replace the SIS as established by the Schengen Convention.

---

2 OJ C , , p. .
3 OJ C , , p. .
4 OJ L 239, 22.9.2000, p. 19. Convention as last amended by Regulation (EC) No 871/2004 (OJ L 162, 30.4.2004, p. 29).
5 OJ L 328 , 13.12.2001, p.4.
6 OJ L 328, 13.12.2001, p. 1.

(3) This Regulation constitutes the necessary legislative basis for governing the SIS II in respect of matters falling within the scope of the Treaty establishing the European Community (hereinafter referred to as the "EC Treaty"). Council Decision No 2006/XX/JHA on the establishment, operation and use of the SIS II[7] constitutes the necessary legislative basis for governing the SIS II in respect of matters falling within the scope of the Treaty of the European Union (hereinafter referred to as the "EU Treaty").

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

(5) The SIS II should constitute a compensatory measure contributing to maintaining a high level of security within an area (…) of freedom, security and justice by supporting the implementation of policies linked to the movement of persons part of the Schengen acquis, as integrated into Title IV of the EC Treaty.

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

(7) The expenditure involved in the operation of the Central SIS II and the Communication Infrastructure should be charged to the budget of the European Union.

(8) It is necessary to establish a manual setting out the detailed rules for the exchange of supplementary information in relation with the action required by the alert. 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 the Central SIS II and of parts of the Communication Infrastructure.

However, in order to ensure a smooth transition between the SIS 1+ and the 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 a financial, operational and organisational perspective, and legislative proposals from the Commission, a permanent Management Authority with responsibility for these tasks should be established. The transitional period should last for no more than five years from the date of entry into force of this Regulation.

---

[7] OJ. L…

(10) The SIS II should contain alerts on refusal of entry or stay. It is (…) necessary to further consider harmonising the provisions on the grounds for issuing alerts to third country nationals for the purpose of refusing entry or stay and to clarifying their use in the framework of asylum, immigration and return policies. Therefore, the Commission should review, three years after the entry into application of this Regulation, the provisions on the objectives and the conditions for issuing alerts for the purpose of refusal of entry or stay.

(11) Alerts aiming at refusing entry or stay should not be kept longer in the SIS II than the time required to meet the purposes for which they were supplied. As a general principle, they should be automatically erased from the SIS II after a period of three years. The decision to keep the alert should be based on a comprehensive individual assessment. Member States should review these alerts within this three year period and keep statistics about the number of alerts the conservation period of which has been extended.

(12) The SIS II should permit the processing of biometric data in order to assist in the reliable identification of individuals concerned. In the same context the SIS II should also allow for the processing of data of 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.

(13) The SIS II should offer Member States the possibility to establish links between alerts. The establishment of links by a Member State between two or more alerts should have no impact on the action to be taken, the conservation period or the access rights to the alerts.

(13A) Data processed in the SIS II in application of this Regulation should not be transferred or made available to a third country or to an international organisation.

(14) Directive 1995/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[8] applies to the processing of personal data carried out in application of this Regulation. This includes the designation of the controller in accordance with Article 2(d) of that Directive and the possibility for Member States to provide for exemptions and restrictions to some of the provided rights and obligations in accordance with Article 13(1) of that Directive including as regards the rights of access and information of the individual concerned. The principles set out in Directive 1995/46/EC should be supplemented or clarified in this Regulation, where necessary.

(15) Regulation (EC) No 2001/45 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

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

the free movement of such data[9] and in particular its Articles 21 and 22 as regards confidentiality and security of the processing applies to the processing of personal data by the Community institutions or bodies when carrying out their tasks as responsible for the operational management of the SIS II. The principles set out in Regulation (EC) No 2001/45) should be supplemented or clarified in this Regulation, where necessary.

(15A) *(moved to Recital 15)*

(15B) 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 shall apply to officials or other servants of the European Communities employed and working in connection with SIS II.

(16) 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 by 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[10], should monitor the activities of the Community institutions and bodies in relation to the processing of personal data taking into account the limited tasks of the Community institutions and bodies with regard to the data themselves.

(17) Liability of the Community arising from any breach by the Community institutions or bodies of this Regulation is governed by the second paragraph of Article 288 of the EC Treaty.

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

(18a) In order to ensure transparency, a report on the technical functioning of the 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 Management Authority. An overall evaluation should be issued by the Commission every four years.

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

9 OJ L 8, 12.1.2001, p. 1.
10 OJ L 12, 17.1.2004, p. 47.

should take into account the smooth operation of national applications. Subject to an impact assessment by the Commission, it will be decided to what extent the implementing measures could be a responsibility of the permanent Management Authority, as soon as it is set up.

(20) The measures necessary for the implementation of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[11] .

(21) It is appropriate to lay down transitional provisions in respect of alerts issued in the SIS 1+ (…) which will be transferred to the 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 the SIS 1+ to the SIS II, as well as any hit on such an alert should trigger an immediate examination of its compatibility with the provisions of this Regulation.

(22) It is necessary to lay down special provisions regarding the remainder of the budget affected to the operations of the SIS which are not part of the budget of the European Union.

(23) 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 Community level, the Community may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to achieve those objectives.

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

(25) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and the Treaty establishing the European Community, Denmark is not taking part in the adoption of this Regulation and is, therefore, not bound by it or subject to its application. Given that this Regulation builds upon the Schengen acquis under the provisions of Title IV of Part Three of the EC Treaty, Denmark shall, in accordance with Article 5 of the said Protocol, decide, within a period of six months after date of the adoption of this Regulation, whether it will implement it in its national law.

[11] OJ L 184, 17.7.1999, p. 23.

(26) This Regulation constitutes a development of provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with 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[12]. The United Kingdom is therefore not taking part in its adoption and is not bound by it or subject to its application.

(27) This Regulation constitutes a development of provisions of the Schengen acquis in which Ireland does not take part, in accordance with 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[13]. Ireland is therefore not taking part in its adoption and is not bound by it or subject to its application.

(27A) This Regulation is without prejudice to the arrangements for the United Kingdom and Ireland's partial participation in the Schengen acquis as defined in Decision 2000/365/EC and Decision 2002/192/EC respectively.

(28) As regards Iceland and Norway, this Regulation 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[14,] which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[15].

(28A) An arrangement has to 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[16], annexed to the abovementioned Agreement.

(29) As regards Switzerland, this Regulation 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

12 OJ L 131, 1.6.2000, p. 43.
13 OJ L 64, 7.3.2002, p. 20.
14 OJ L 176, 10.7.1999, p. 6.
15 OJ L 176, 10.7.1999, p. 31.
16 OJ L 176, 10.7.1999, p. 53.

read in conjunction with Article 4(1) of Council Decisions 2004/849/EC[17] and 2004/860/EC[18].

(29A) An arrangement has to 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.[19]

(30) This Regulation 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.

(31) This Regulation should apply to the States concerned by Recitals 29 and 30 on dates determined in accordance with the procedures set out in the relevant instruments concerning the application of the Schengen acquis to those States.

CHAPTER I
General provisions

1. Article 1
2. Establishment and general objective of the SIS II

1. The second generation Schengen Information System (hereinafter referred to as "SIS II") is hereby established.

3.

2. The purpose of the SIS II shall be, in accordance with this Decision, to ensure a high level of security within an area (…) of freedom, security and justice, 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 the Treaty establishing the European Community (hereinafter referred to as "EC Treaty") relating to the movement of persons in their territories, using information communicated via this system.

---

17 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).

18 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).

19 Provisional insertion, pending a permanent solution to this question.

4. Article 2
5. Scope

1. This Regulation defines the conditions and procedures for the processing of alerts entered in the SIS II in respect of third country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry or stay in the territory of the Member States.

2. This Regulation also lays down provisions in particular on the technical architecture of the SIS II, the responsibilities of the Member States and of the Management Authority referred to in Article 12, general data processing, the rights of the persons concerned and liability.

6. Article 3
7. Definitions

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

   a. "alert" means a set of data entered in the SIS II allowing the competent authorities to identify a person (…) in view of a specific action to be taken;

   b. "supplementary information" means the information not stored in the SIS II, but connected to SIS II alerts, which shall be exchanged:

      a. in order to allow Member States to consult or inform each other whilst entering an alert;

      b. following a hit in order to allow the appropriate action to be taken;

      c. when the required action cannot be taken;

      d. when dealing with the quality of SIS II data;

      e. when dealing with the compatibility and priority of alerts;

      f. when dealing with the exercise of the right of access;

   c. "additional data" means the data stored in the SIS II and connected to SIS II alerts which shall be immediately available to the competent authorities where persons in respect of whom data has been entered in the SIS II are found as a result of searches made therein;

   d. "third country national" means any individual who is not:

      a. (…) a citizen of the European Union within the meaning of Article 17(1) of the EC Treaty; or

b. (…) a national of a third country who, under agreements between the Community and its Member States on the one hand, and these countries, on the other, enjoys rights of free movement equivalent to those of citizens of the Union.

e. personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly;

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

8. Article 4

9. Technical architecture and ways of operating the SIS II

1. The SIS II is composed of:

(aa) a central system (hereinafter referred to as "the Central SIS II") composed of:

- a technical support function (hereinafter referred to as "CS-SIS") containing the (…) SIS II database;

- a uniform national interface (hereinafter referred to as "NI-SIS");

(a) a national section (hereinafter referred to as "N.SIS II") in each of the Member States, consisting of the national data systems which communicate with the Central SIS II. An N.SIS II may contain a data file (hereinafter referred to as "national copy"), containing a complete or partial copy of the (…) SIS II database;

(b) *(moved to (aa))*

(c) a communication infrastructure between the CS-SIS and the NI-SIS (hereinafter referred to as "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 N.SIS II. 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. The principal CS-SIS, which carries out technical supervision and administration, is located in Strasbourg (France) and a backup CS-SIS, capable

of ensuring all functionalities of the principal CS-SIS in case of failure of this system, is located in Sankt Johann im Pongau (Austria).

4. The CS-SIS will provide the services necessary for the update of, and searches in, the (…) SIS II database. For the Member States which use a national copy the CS-SIS will provide:

   1. the on-line update of the national copies;

   2. the synchronisation and the coherence between the national copies and the (…) SIS II database;

   3. the operation for initialisation and restoration of the national copies.

10.

11. Article 5
12. Costs

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

2. These costs will include work done with respect to the 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.

4. *(…)*

CHAPTER II
Responsibilities of the Member States

13. Article 6
14. National Systems

Each Member State (…) shall be responsible for:

(a) setting up, operating and maintaining its N.SIS II;

(b) connecting its N.SIS II to the NI-SIS.

15.

16. Article 7
17. N.SIS II Office and SIRENE Bureau

1. (a) Each Member State shall designate an authority (hereinafter referred to as "N.SIS II Office"), which shall have central responsibility for its N.SIS II;

(b) The said 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 Regulation;

(c) Each Member State shall transmit its alerts via the N.SIS II Office.

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

(b) This Bureau shall also coordinate the verification of the quality of the information entered in the SIS II (…);

(c) For those purposes it shall have access to data processed in the SIS II.

3. The Member States shall inform the Management Authority referred to in Article 12 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 21(6).

18. Article 8
19. Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure.

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

3. Should the Communication Infrastructure be unavailable, Member States may use other adequately secured technical means for exchanging supplementary information.

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

3a Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 35(3) in the form of a manual called the "SIRENE Manual", without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

20. Article 9
21. Technical compliance

1. To ensure the rapid 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 the CS-SIS with the N.SIS II. These

protocols and technical procedures shall be established in accordance with the procedure referred to in Article 35(3), without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12 (…).

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

22. Article 10
23. Security (...)

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

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

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

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

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

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

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

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

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

g. 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);

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

(ha) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure the compliance with this Regulation (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 10 A
Confidentiality

Each Member State shall apply its rules of professional secrecy or other equivalent obligations 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.

24. Article 11
25. Keeping of records at national level

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

(b) 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(a), with the exception of exchanges connected to the services referred to in Article 4(4).

1a *(moved to 1(b))*

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 a search, the reference to the data transmitted and the name of both the competent authority and the person responsible for processing the data.

3. The records may only be used for the purpose specified in paragraph 1 and shall be deleted at the earliest after a period of one year and at the latest after a period of three years after their creation. The records which include the history of alerts shall be erased after a period of one to three years after the deletion of the alerts.
4. Records may be kept longer if they are required for monitoring procedures which have already begun.
4a The competent national authorities in charge of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning of the N.SIS II, data integrity and security, shall have access, within the limits of their competence and upon request, to these records to ensure that they are able to fulfil their tasks.

26. Article 11 A
27. Self-monitoring

The Member States shall (…) ensure that each authority entitled to access SIS II data shall take the measures necessary to ensure compliance with this Regulation and shall cooperate, where necessary, with the National Supervisory Authority, as referred to in Article 31(1a).

28. Article 11 B
29. Staff training

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

30. Article 11 C
31. Communication with the public

(deleted)

Chapter III(…)
Responsibilities of the Management Authority

Article 12
Operational management

1. A Management Authority, which shall be funded by the budget of the European Union, shall be responsible for the operational management of the Central SIS II. It shall also be responsible for the following tasks related to the Communication Infrastructure:

(a) supervision;

(b) security;

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

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

(a) budget implementing tasks;

(b) acquisition and renewal;

(c) contractual matters.

3. During a transitional period before the Management Authority mentioned in paragraph 1 takes up its responsibilities, the Commission shall be responsible for the operational management of the Central SIS II. The Commission may entrust the exercise of this management as well as of budget implementing tasks, 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[20], to national public sector bodies, in two different countries.

3aa Each national public sector body, as referred to in paragraph 3, must comply in particular with the following selection criteria:

a. it must demonstrate a long term experience in operating a large-scale information system with the functionalities referred to in Article 4(4);

b. it must possess a long term expertise in the service and security requirements of an information system comparable to the functionalities 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 provided for in Article 4;

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

e. it must work in an administrative environment allowing it to implement its tasks properly and avoid any conflict of interests.

3a The Commission shall prior to any such delegation and at regular intervals afterwards inform the European Parliament and the Council about the conditions of delegation, the precise scope of the delegation, and the bodies to which tasks are delegated.

---

[20] Official Journal L 248 of 16/09/2002, p. 1-48.

3b In case the Commission delegates its responsibility during the transitional period (…) pursuant to paragraph 3 it shall ensure that this delegation fully respects the limits set by the institutional system laid out in the Treaty. It shall ensure, in particular, that this delegation does not adversely affect any effective control mechanism under (…) Community law, be it by the Court of Justice, the Court of Auditors or the European Data Protection Supervisor.

4. Operational management of the Central SIS II shall consist of all the tasks necessary to keep the Central SIS II functioning on a 24 hours a day, 7 days a week basis in accordance with this Regulation, in particular the maintenance work and technical developments necessary for the smooth running of the system.

5. *(deleted)*

6. 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 the Central SIS II.

32. Article 13
33. Security (...)

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

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

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

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

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

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

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

(ea) 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 without delay upon its request (personnel profiles);

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

(fa) 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);

g. 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);

(ga) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure the compliance with this Regulation (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 13 A
Confidentiality

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 obligations of confidentiality to all its staff required to work with SIS II data on comparable standards to those provided in Article 10 A. 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.

34. Article 14
35. Keeping of records at central level

1. The Management Authority shall ensure that every access to and all exchanges of personal data within the CS-SIS are recorded for the purposes provided for in Article 11(1).

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 a search, the reference to the

data transmitted and the identification of the competent authority responsible for processing the data.

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

4. Records may be kept longer if they are required for monitoring procedures which have already begun.

4a The competent authorities in charge of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning of the CS-SIS, data integrity and security, shall have access, within the limits of their competence and upon request, to these records to ensure that they are able to fulfil their tasks.

36. Article 14 AA
37. Information campaign

The Commission shall, in co-operation with the National Supervisory Authorities, referred to in Article 31(1a), and the European Data Protection Supervisor, referred to in Article 31A(1), accompany the start of the operation of the SIS II with an information campaign informing the public about the objectives, the data stored, the authorities with access and the rights of persons. After its establishment, the Management Authority, in co-operation 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 in general about the SIS II.

Chapter IV
Alerts issued in respect of third country nationals for the purpose of refusing entry and stay

38. Article 14 A (…)
39. Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, the 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 Article 15.

2. The information on (…) persons for whom an alert has been issued shall be no more than the following:

a. surname(s) and forename(s), name at birth and previously used names and any aliases possibly 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 persons concerned are armed, violent or have 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 the SIS II pursuant to Article 26.

3. (…)

3a 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 35(3), without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

3b. The technical rules necessary for searching the data referred to in paragraph 3a shall be similar for searches in the CS-SIS, in national copies and in technical copies, as referred to in Article 21(2).

40.

41. Article 14 B
42. Proportionality clause

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

43. Article 14 C
44. Specific rules for photographs and fingerprints

Photographs and fingerprints as referred to in Article 14 A(2)(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 35(3), without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

(b) Photographs and fingerprints shall only be used to confirm the identity of a third country national who has been found as a result of an alphanumeric search made in the SIS II.

(c) As soon as technically possible, fingerprints may also be used to identify a third country national on the basis of his/her biometric identifier. Before this functionality is implemented in the 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.

45.

46. Article 14 D
47. Requirement for an alert to be entered

1. An alert cannot be entered without the data referred to in Articles 14 A(2)(a), 14 A(2)(d), 14 A(2)(k) and 14 A(2)(l).

2. In addition, when available, all other data listed in Article 14 A(2) shall be entered.

48.

49. Article 15
50. Conditions for issuing alerts on refusal of entry or stay

1. Data on third country nationals for whom an alert has been issued for the purposes of refusing entry or stay shall be entered on the basis of a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law. This decision may only be taken on the basis of an individual assessment. (…) Appeals against these decisions shall be carried out in accordance with national legislation.

1a *(deleted)*

2. An alert shall be entered when the decision referred to in paragraph 1 was based on a threat to public policy or public security or to national security which the presence of a third country national in national territory may pose. This situation shall arise in particular in the case of:

a. a third country national who has been convicted of an offence by a Member State carrying a penalty involving deprivation of liberty of at least one year;

b. a third country national in respect of whom there are serious grounds for believing that he has committed serious criminal offences or in respect of whom there are clear indications of an intention to commit such offences in the territory of a Member State;

c. *(moved to Article 15 AA)*

2a *(moved to Article 15 A)*

3. An alert may also be entered when the decision referred to in paragraph 1 was based on the fact that the third country national has been subject to measures involving expulsion, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third country nationals.

3a *(moved to paragraph 1)*

3b This Article does not apply in respect of the persons referred to in Article 15 AA.

3c The application of (…) this Article (…) shall be reviewed by the Commission three years after the date referred to in Article 39(2). Based on this review the Commission shall, using its right of initiative in accordance with the Treaty, make the necessary proposals to modify the provisions of this Article (…) to achieve a higher level of harmonisation of the criteria for entering alerts.

51.
52. Article 15 A
53. Conditions for entering alerts on third country nationals
54. who are beneficiaries of the Community right of free movement

1. An alert concerning a third country national who is a beneficiary of the Community right of free movement within the meaning of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States shall be based in conformity with rules adopted in implementing the Directive.

2. In case of a hit on an alert pursuant to Article 15 concerning a third country national who is a beneficiary of the Community right of free movement, the executing Member State shall consult immediately the issuing Member State, by means of its SIRENE Bureau and in accordance with the provisions of the SIRENE Manual, in order to decide without delay on the action to be taken.

Article 15 AA
55. Conditions for issuing alerts on third country nationals
56. subject to a restrictive measure taken in accordance with Article 15 TEU

1. Without prejudice to Article 15 A, third country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the EU Treaty including those implementing a travel ban issued by the Security Council of the United Nations, shall, insofar as data quality requirements may be satisfied, be entered into the SIS II for the purpose of refusing entry or stay.

2. Art 14D shall not apply in respect of alerts entered on the basis of paragraph 1.

3. The Member State that shall enter, update and delete these alerts on behalf of all Member States shall be designated at the moment of the adoption of the relevant measure taken in accordance with Article 15 of the Treaty on the European Union.

57. Article 16
58. Categories of data

(…)

59.

60. Article 17
61. Authorities with the right to access (…) alerts

1. Access to data entered in the SIS II in accordance with Article 15 and the right to search such data directly or in a copy of data of the CS-SIS shall be reserved exclusively to the authorities responsible for the identification of third country nationals for:

   a. border control, in accordance with Regulation 562/2006/EC 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);

   b. other police and customs checks carried out within the country, and the coordination of such checks by designated authorities.

2. However, access to data entered in the SIS II and the right to search such data directly may also be exercised by national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation, as well as their coordination authorities.

3. In addition, access to data entered in accordance with Article 15 and the data concerning documents relating to persons entered in accordance with Article 35(2)(d) and (e) of Council Decision 2006/XX and the right to search such data

directly may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation on third country nationals in the context of the application of the Community acquis relating to the movement of persons. Access to data by these authorities shall be governed by the national law of each Member State.

4. The authorities referred to in this Article shall be included in the list referred to in Article 21(6).

62. Article 17 A
63. Limits of access

Users may only access data which they require for the performance of their tasks.

64.

65. Article 18

(…)

66.
67. Article 18 A

(…)
68.

69.
70. Article 19
71. Access to alerts on identity documents

(…)

72.
73.
74. Article 20
75. Conservation period of the alerts

1. Alerts on persons entered into the SIS II pursuant to this Regulation shall be kept only for the time required to meet the purposes for which they were supplied.
(… moved to paragraph 2)

2. Within three years from entering such an alert into the SIS II the necessity of keeping the alert shall be reviewed by the Member State issuing it.

2aa Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

2a The Member State issuing the alert may, within the review period, decide, following an comprehensive individual assessment, which shall be (…) recorded, to keep the alert should this prove necessary for the purposes for which the alert was issued. In this case paragraph 2 applies accordingly. Any extension of the alert must be communicated to the CS-SIS.

3. Alerts shall automatically be erased after the reviewing period referred to in paragraph 2 has expired. This will not apply in case the Member State issuing the alert communicated the extension of the alert to the CS-SIS as referred to in paragraph 2a. The CS-SIS shall automatically inform the Member States of scheduled deletion of data from the system four months in advance.

4. *(moved to paragraph 3)*

4a *(moved to Article 20 AA)*

4b Member States shall keep statistics about the number of alerts the conservation period of which has been extended in accordance with paragraph 2a.

76.

77. Article 20 AA
78. Acquisition of citizenship and alerts on refusal of entry

Alerts issued in respect of a person who has acquired citizenship of any State whose nationals are beneficiaries of the Community right of free movement shall be erased as soon as the Member State which issued the alert is informed pursuant to Article 24 or becomes aware that the person has acquired such citizenship.

79.

80. Article 20 A
81. Extension of the conservation period of the alerts

(deleted)

CHAPTER V
General data processing rules

82. Article 21
83. Processing of SIS II data

1. The Member States may process the data provided for in Article 15 for the purposes of refusing entry or stay in their territories.

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 17 to carry out a direct search. The provisions of this Regulation shall apply to these copies. Alerts issued by other Member States may not be copied from the N.SIS II into other national data files.

2a (a) Technical copies, as referred to in paragraph 2, which lead to off-line databases may only be created for a period that shall not exceed 48 hours. This duration may be extended in emergency situations. These copies shall be destroyed once the emergency situation comes to an end.

(aa) By way of derogation to paragraph (a), technical copies which lead to off-line databases to be used by visa issuing authorities shall not be authorised one year after the authority in question has been connected successfully to the Communication Infrastructure for the Visa Information System as referred to in Regulation xx/xxxx/EC concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas. This shall not apply to copies made to be used only in emergency situations following the unavailability of the network for more than 24 hours.

(b) (...) Member States shall keep an up-to-date inventory of these copies, make this inventory available to National Supervisory Authorities, as referred to in Article 31(1a) and ensure that the provisions of this Regulation, in particular those referred to in Article 10, are applied in respect of these copies.

3. Access to SIS II data shall only be authorised within the limits of the competence of the national authority and to duly authorised staff.

3a Data may not be used for administrative purposes. By way of derogation, data entered under this Regulation may be used in accordance with national law of each Member State by the authorities referred to in Article 17(3) for the performance of their tasks.

4. Data entered under Article 15 and data concerning documents relating to persons entered under Article 35(2)(d) and (e) of Council Decision xx/xxxx may be used in accordance with the national law of each Member State for the purposes referred to in Article 17(3).

5. Any use of data which does not comply with paragraphs 1 to 4 shall be considered as misuse under the national law of each Member State.

6. Each Member State shall send to the Management Authority a list of competent authorities which are authorised to search the data contained in the SIS II directly pursuant to this Regulation and any changes thereto. That 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.

84. Article 22
85. Entering a reference number

(…)

86.

87. Article 23
88. SIS II data and national files

1. Article 21 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 21(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert, which that Member State has issued in the SIS II.

89.

90. Article 23 A
91. SIS II alerts and national law

1. *(…)*

2. Insofar as (…) Community law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS II.

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

92. Article 24
93. Quality of the data processed in the SIS II (…)

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

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

3. If one of the Member States which has not issued the 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 issuing the alert thereof at the earliest opportunity and not later than ten days after the said evidence has come to its attention; the latter 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 case to the European Data Protection Supervisor who shall jointly with the involved National Supervisory Authorities, as referred to in Article 31, act as mediator.

5. *(…)*

5a The Member States shall exchange supplementary information if a person claims not to be the person wanted by an alert. If the outcome of the check is that there are in fact two different persons this person shall be informed about the provisions referred to in Article 25.

Where a person is already the subject of an alert in the 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. (…)

94.

95. Article 24 A

96. Distinguishing between persons with similar characteristics

1. When, while introducing a new alert, it appears that there is already a person in the SIS II with the same identity description element, the following procedure shall be followed:

2. *(deleted)*

   a. *(deleted)*

   b. the SIRENE bureau shall contact the requesting department to clarify whether the alert is on the same person or not;

   c. if the cross-check reveals that the person in question is indeed one and the same, the SIRENE bureau shall apply the procedure for entering multiple alerts as referred to in Article 24(6). If the outcome of the check is that there are in fact two different people, the SIRENE bureau approves the request for entering another alert by adding the necessary elements to avoid any misidentifications.

97.

98. Article 25

99. Additional data for the purpose of dealing with misused identity

1. Where confusion may arise between the person actually intended by 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 related to the latter to the alert in order to avoid the negative consequences of misidentifications.

2. The data related to a person whose identity has been misused shall only be used for the following purposes:

   a. to allow the competent authority to differentiate the person whose identity has been misused from the person actually intended by 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. No more than the following personal data may be entered and further processed in the SIS II for the purpose of this article:

a) surname(s) and forename(s), name 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 issuing.

3a The technical rules necessary for entering, updating and deleting the data referred to in paragraph 3 shall be established in accordance with the procedure referred to in Article 35(3), without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

4. 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.

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

100.

101. Article 26

102. Links between alerts

1. A Member State may create a link between alerts it issues in the 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 conservation period of each of the linked alerts.

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

3a A Member State shall create a link between alerts only when there is a clear operational need.

3b 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.

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

4a. The technical rules for linking alerts shall be adopted in accordance with the procedure defined in Article 35(3), without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

103.

104. Article 27

105. Purpose and conservation period of supplementary information

1. Member States shall keep a reference to the decisions giving rise to the 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 alert related to the person concerned has been deleted from the 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 of time for which such data may be held in such files shall be governed by national law.

Article 27 AA
Transfer of personal data to third parties

Data processed in the SIS II in application of this Regulation shall not be transferred or made available to a third country or to an international organisation.

CHAPTER VI
Data protection

106. Article 27 A
Processing of sensitive categories of data

Processing of the categories of data listed in Article 8(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data shall not be authorised.

107.

Article 28

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

1. The right of persons to have access to data entered in the SIS II in accordance with this Regulation which relate to them shall be exercised in accordance with the law of the Member State before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 31(1) shall decide whether information shall be communicated and by what procedures. A Member State which has not issued the alert may communicate information concerning such data only if it has previously given the Member State issuing the alert an opportunity to state its position. This shall be done through the exchange of supplementary information.

2. Communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the 2. protection of the rights and freedoms of third parties.

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

3a 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. If national law provides for a shorter delay, the latter shall be respected.

3b 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 3 months from the date on which he applies for correction or deletion. If national law provides for a shorter delay, the latter shall be respected.

109.

110. Article 29

111. Right of information

1. Third country nationals who are the subject of an alert issued in accordance with this Regulation shall be informed in accordance with Article 10 and 11 of Directive 95/46/EC.This information shall be provided in writing, together with a copy of or a reference to the national decision, referred to in Article 15(1), giving rise to the alert.

2. This information shall in any case not be provided:

   a. where

      i. the personal data have not been obtained from the third country national in question; and

      ii. the provision of the information proves impossible or would involve a disproportionate effort;

b. where the third country national in question already has the information;

c. where, (…) national law allows for a restriction to the right of information (…),in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

3. (…)

112. Article 30
113. Remedies

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

114.

115. 2. The Member States undertake mutually to enforce final decisions taken by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 32.

116.

117. 3. The rules on remedies provided for in this Article shall be evaluated by the Commission two years after the entry into force of this Regulation.

118. Article 31
119. Supervision of the N.SIS II

1a. The authority or authorities designated in each Member State and endowed with the powers referred to in Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the "National Supervisory Authorities") shall monitor independently the lawfulness of the processing of SIS II personal data on and from their territory, including the exchange and further processing of supplementary information.

1b. The authority or authorities referred to in paragraph 1a shall ensure that at least every four years an audit of the data processing operations in the N.SIS II is carried out according to international auditing standards.

1c. Member States shall ensure that the authority or authorities referred to in paragraph 1a have sufficient resources to fulfil the tasks entrusted to them by this Regulation.

2. *(…)*

3. *(…)*

4. *(…)*

5. *(…)*

6. *(…)*

7. *(…)*

120. Article 31 A

121. Supervision of the Management Authority

1. The European Data Protection Supervisor shall monitor that the personal data processing activities of the Management Authority are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of 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 shall apply accordingly.

2. The European Data Protection Supervisor shall ensure that at least every four years an audit of the Management Authority's personal data processing activities is carried out according to international auditing standards. The report of the 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.

122. Article 31 B

123. Cooperation between National Supervisory Authorities and the EDPS

1. The National Supervisory Authorities (…) and the European Data Protection Supervisor, each acting within the scope of their 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 their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as may be needed.

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 at the charge of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly according to need. A joint

report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years.

124. Article 31 C
125. Data protection during the transitional period

In case the Commission delegates its responsibilities during the transitional period to another body, pursuant to Article 12(3), it shall ensure that the European Data Protection Supervisor shall have the right and possibility to fully exercise his tasks including the possibility to carry out checks on the spot or to exercise (…) any other powers endowed to the European Data Protection Supervisor by Article 47 of 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**.**

CHAPTER VII
Liability and sanctions
126.
127. Article 32
128. Liability

1. Each Member State shall be liable in accordance with its national law for any injury caused to a person through the use of the N.SIS II. This shall also apply to injury 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 data were used by the Member State requesting reimbursement in breach of this Regulation.

3. If failure of a Member State to comply with its obligations under this Regulation causes damage to the SIS II, that Member State shall be held liable for such damage, unless and insofar as the Management Authority or other Member State(s) participating in the SIS II failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

129.

130. Article 33
131. Sanctions

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

CHAPTER VIII
Final Provisions

132. Article 34
133. Monitoring and statistics

1. The Management Authority shall ensure that procedures are in place to monitor the functioning of the SIS II against objectives, in terms of 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 related to the processing operations performed in the Central SIS II.

2a 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 the SIS II was accessed, respectively given as a total and for each Member State.

3. Two years after the SIS II starts operations and every two years thereafter, the Management Authority shall submit to the European Parliament and the Council a report on the technical functioning of the Central SIS II and the Communication Infrastructure, including its security, the bilateral and multilateral exchange of supplementary information between Member States.

4. Three years after the SIS II starts operations and every four years thereafter, the Commission shall produce an overall evaluation of the Central SIS II and the bilateral and multilateral exchange of supplementary information between Member States. This overall evaluation shall include the examination of results achieved against objectives, assess the continuing validity of the underlying rationale, the application of this Regulation in respect of the Central SIS II, the security of the Central SIS II and any implications of future operations. The Commission shall transmit the reports on the evaluation to the European Parliament and the Council.

5. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraph 2a, 3 and 4.

5a. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 4.

6. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for producing and submitting the reports referred to in paragraphs 2a and 3.

134. Article 35
135. Committee

1. The Commission shall be assisted by a Committee.

2. *(deleted)*

3. Where reference is made to this paragraph, the regulatory procedure laid down in Article 5 of Decision 1999/468/EC shall apply, in compliance with Article 7(3) thereof. The period provided for in Article 5(6) of Decision 1999/468/EC shall be three months.

4. The Committee shall adopt its Rules of Procedure.

5. The Committee referred to in paragraph 1 shall exercise its function from the date of entry into force of this Regulation.

136. Article 36
137. Amendment of the provisions of the Schengen Acquis

1. For the purposes of matters falling within the scope of the EC Treaty, this Regulation replaces, on the date referred to in Article 39(1a), the provisions of Articles 92 to 119 of the Schengen Convention, with the exception of Article 102 A thereof.

2. It also replaces, on the date referred to in Article 39(1a), the following provisions of the Schengen acquis implementing those articles[21] :

   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 28 April 1999 on C.SIS installation expenditure (SCH/Com-ex (99) 4);

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

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

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

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

i. 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 EC 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 Regulation and shall be read in accordance with the correlation table set out in the Annex.

138. Article 37
139. Repeal

Regulation (EC) No 378/2004, Regulation (EC) No 871/2004, Decision 2005/451/JHA, Decision 2005/728/JHA and Decision 2006/628/EC are repealed on the date referred to in Article 39(1a).

140.

141. Article 38
142. Transitional period and budget

1. Alerts may be transferred from SIS 1+ to the SIS II. The Member States shall ensure, giving priority to alerts on persons, that the contents of the alerts that are transferred from the SIS 1+ to the SIS II satisfy the provisions of this Regulation as soon as possible and within three years of the date referred to in Article 39(1a) at the latest. During this transitional period, the Member States may continue to apply the provisions of Articles 94 and 96 (…) of the Schengen Convention (…) to the contents of the alerts that are transferred from the SIS 1+ to the SIS II, subject to the following rules:

- In the event of a modification of, an addition to or a correction or update of the content of an alert transferred from the SIS 1+ to the SIS II, the Member States shall ensure that the alert satisfies the provisions of this Regulation as from the time of that modification, addition, correction or update.

- In the event of a hit on an alert transferred from the SIS 1+ to the SIS II, the Member States shall examine the compatibility of that alert with the provisions of this regulation 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 39(1a), 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 12(3), references in this Regulation to the Management Authority shall be construed as a reference to the Commission.

143.

144. Article 39

Entry into force, applicability and migration

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

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

2. The date referred to in paragraph 1a shall be fixed after:

a) the necessary implementing measures have been adopted;

b) all Member States fully participating in the 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 the 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. This validation will confirm that the level of performance of the SIS II is at least equivalent to that achieved with SIS 1+;

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

2a The Commission shall inform the European Parliament of the results of the tests carried out according to paragraph 2(c).

3. Any Decision of the Council taken in accordance with paragraph 1a shall be published in the Official Journal of the European Union.

4. *(deleted)*

145. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at Strasbourg,

For the European Parliament
The President

For the Council
The President

ANNEX

Correlation table

Schengen Convention[22] Articles	**Regulation Articles**
Art. 92(1)	Art. 1(1); Art. 2(1); Art. 4(1)(2)(3)
Art. 92(2)	Art. 4(1)(2)(3); Art. 5(2)(3); Art.6; Art.9
Art. 92(3)	Art. 4(1)(2)(3), Art. 5(1), Art. 12
Art. 92(4)	Art.3 (1); Art. 7(2)(3); Art.8
Art. 93	Art.1(2)
Art. 94(1)	Art. 21(1)
Art. 94(2)	Art.15(1)
Art. 94(3)	Art. 16(1); Art. 25(3)
Art. 94(4)	
Art. 95(1)	
Art. 95(2)	
Art. 95(3)	
Art. 95(4)	
Art. 95(5)	
Art. 95(6)	
Art. 96(1)	Art. 15(1)
Art. 96(2)	Art. 15(1)
Art. 96(3)	Art. 15(1)
Art. 97	
Art. 98(1)	
Art. 98(2)	
Art. 99(1)	
Art. 99(2)	
Art. 99(3)	
Art. 99(4)	
Art. 99(5)	
Art. 99(6)	
Art. 100(1)	
Art. 100(2)	
Art. 100(3)	
Art. 101(1)	Art. 17(1)
Art. 101(2)	Art. 17(1)(3); Art. 18; Art.19
Art. 101(3)	Art. 21(2)
Art. 101(4)	Art. 21(3)
Art. 101A(1)	
Art. 101A(2)	
Art. 101A(3)	
Art. 101A(4)	
Art. 101A(5)	
Art. 101A(6)	
Art. 101B(1)	

[22] Articles and paragraphs in italics have been added or amended by Council Regulation (EC) No. 871/2004 and Council Decision 2005/211/JHA on the introduction of new functions for the Schengen Information System, including the fight against terrorism.

Schengen Convention[22] Articles	Regulation Articles
Art. 101B(2)	
Art. 101B(3)	
Art. 101B(4)	
Art. 101B(5)	
Art. 101B(6)	
Art. 101B(7)	
Art. 101B(8)	
Art. 102(1)	Art. 21(1)
Art. 102(2)	Art. 23(1)(2)
Art. 102(3)	
Art. 102(4)	Art.17(1)(3); Art.18; Art.19
Art. 102(5)	Art. 32(1)
Art. 103	Art. 11
Art. 104(1)	
Art. 104(2)	
Art. 104(3)	
Art. 105	Art. 24(1)
Art. 106(1)	Art. 24(2)
Art. 106(2)	Art. 24(3)
Art. 106(3)	Art. 24(4)
Art. 107	Art. 24(6)
Art. 108(1)	Art. 7(1)
Art. 108(2)	
Art. 108(3)	Art. 6; Art. 7(1); Art. 9(1)
Art. 108(4)	Art. 7(3)
Art. 109(1)	Art. 28; Art. 29(1)(2)(3)
Art. 109(2)	
Art. 110	Art. 29(1)(4); Art.31(1)
Art. 111(1)	Art. 30
Art. 111(2)	
Art. 112(1)	Art. 20(1)(2)(3)(4)(5); Art. 24(7)
Art. 112(2)	Art. 24(7)
Art. 112(3)	Art. 20(6)
Art. 112(4)	Art.20(5)
Art. 112A(1)	Art. 27(2)
Art. 112A(2)	Art. 27(3)
Art. 113(1)	
Art. 113(2)	Art. 14(3)(4)(5)(6)
Art. 113A(1)	Art. 27(2)
Art. 113A(2)	Art. 27(3)
Art. 114(1)	Art. 31(1)
Art. 114(2)	Art. 31
Art. 115(1)	Art. 31(2)
Art. 115(2)	
Art. 115(3)	
Art. 115(4)	
Art. 116(1)	Art. 32(1)

Schengen Convention[22] Articles	Regulation Articles
Art. 116(2)	Art. 32(2)
Art. 117(1)	
Art. 117(2)	
Art. 118(1)	Art. 10(1)
Art. 118(2)	Art. 10(1)
Art. 118(3)	Art. 10(3)
Art. 118(4)	Art. 13
Art. 119(1)	Art. 5(1); Art.38(2)
Art. 119(2)	Art. 5(2)(3)

P6_TA-PROV(2006)0446

Access to SIS II by the services responsible for issuing vehicle registration certificates ***I

European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing registration certificates for vehicles (COM(2005)0237 – C6-0175/2005 – 2005/0104(COD))

(Codecision procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to the European Parliament and the Council (COM(2005)0237)[23],

– having regard to Article 251(2) and Article 71 of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0175/2005),

– having regard to Rule 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0354/2006),

1. Approves the Commission proposal as amended;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council and Commission.

[23] Not yet published in OJ.

PROPOSAL FOR A REGULATION

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

1. regarding the access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing registration certificates for vehicles

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 71 thereof,

Having regard to the proposal from the Commission[24],

Having regard to the opinion of the European Economic and Social Committee[25],

Having regard to the opinion of the Committee of the Regions[26],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[27],

Whereas:

(1) Article 9 of Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles[28] provides that Member States are to assist one another in the implementation of that Directive and may exchange information at bilateral or multilateral level, in particular, so as to check, before any registration of a vehicle, the latter's legal status, in the Member State in which it was previously registered. Such checking may involve the use of an electronic network.

(2) Regulation XX/2006/EC of the European Parliament and of the Council[29] and Council Decision 2006/XX/JHA[30] on the establishment, operation and use of the second generation of the Schengen Information System (hereinafter "SIS II") constitute the legislative basis for governing the SIS II, which constitutes a shared database between Member States containing, inter alia, data on motor

---

24 OJ C , , p. .
25 OJ C , , p. .
26 OJ C , , p. .
27 OJ C , , p. .
28 OJ L 138, 1.6.1999, p. 57. Directive as last amended by Commission Directive 2003/127/EC (OJ L 10, 16.1.2004, p.29).
29 OJ L…
30 OJ L…

vehicles with a cylinder capacity exceeding 50 cc (…), data on trailers with an unladen weight exceeding 750 kg and caravans (…) and data on vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated.

(3) Regulation XX/2006/EC and Decision 2006/XX/JHA replaced Articles 92 to 119 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 on the gradual abolition of checks at common borders[31] (hereinafter referred to as "the Schengen Convention") with the exception of Articles 102a thereof. That article concerns access to the Schengen Information System by the authorities and services in the Member States responsible for issuing registration certificates for vehicles.

(4) It is now necessary to adopt a third instrument, based on Title V of the EC Treaty and complementing Regulation XX/2006/EC and Decision 2006/XX/JHA in order to allow access to the SIS II by the services in the Member States responsible for issuing registration certificates for vehicles, and to replace Article 102a of the Schengen Convention.

(5) Alerts on objects including motor vehicles are entered in the SIS II for the purposes of seizure or use as evidence in criminal proceedings, pursuant to Decision 2006/XX/JHA.

(6) According to Decision 2006/XX/JHA, access to alerts on objects entered in the SIS II is reserved exclusively to the authorities responsible for police, border and custom authorities, as well as judicial authorities and Europol.

(7) Government or non-government services clearly identified for this purpose and responsible in the Member States for issuing registration certificates for vehicles should have access to data included in the SIS II concerning motor vehicles with a cylinder capacity exceeding 50cc, trailers with an unladen weight exceeding 750 kg, (…) caravans and vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated in order to enable them to check whether the vehicles
presented to them for registration have been stolen misappropriated or lost.

(8) To that end it is necessary to grant those services access to that data, and to allow them to use the data for the administrative purposes of properly issuing vehicle registration certificates.

(9) To the extent that services in the Member States responsible for issuing registration certificates for vehicles are non-government bodies, such access should be granted indirectly, that is to say through the intermediary of an authority granted access in accordance with Decision 2006/XX/JHA,

---

[31] OJ L 239, 22.9.2000, p. 19. Convention as last amended by Regulation (EC) No 871/2004 (OJ L 162, 30.4.2004, p. 29) and Decision 2005/211/JHA (OJ L 68, 15.3.2005, p. 44).

responsible for ensuring compliance with the security and confidentiality rules of the Member States as referred to in Article 10 of this Decision.

(10) Decision 2006/XX/JHA, in particular Article 36 thereof**,** defines the action to be taken if an access to SIS II brings to light an alert for an object entered in the System.

(11) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[32] applies to the processing of personal data by the services in the Member States responsible for issuing registration certificates for vehicles. The specific provisions on the protection of personal data on security, confidentiality and keeping of log files contained in Decision 2006/XX/JHA supplement or clarify the principles set out in that Directive when personal data is processed by those services in the context of SIS II.

(12) Since the objective of the action to be taken, namely to grant access to the SIS II for services in the Member States responsible for issuing registration certificates, in order to facilitate their tasks under Directive 1999/37/EC, cannot be sufficiently achieved by the Member States and can therefore, by reason of the very nature of the SIS as a joint information system, only be achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(12A) This Regulation respects the fundamental rights and observes the principles recognised, in particular by the Charter of Fundamental Rights of the European Union.

(13) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application 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.[33]

(14) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation on 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 Council Decision 1999/437/EC read in conjunction with Article 4 (1) of Council Decision

---

[32] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p.1).

[33] OJ L 176, 10.7.1999, p. 31.

2004/860/EC on the signing, on behalf of the European Community, and on the provisional application of certain provisions of this Agreement[34] and with Article 4 (1) of Council Decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of this Agreement[35].

(15) This Regulation 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,

HAVE ADOPTED THIS REGULATION:

Article 1

1. Notwithstanding Articles 35, 37 and 40 (1) of Decision 2006/XX/JHA, the services in the Member States responsible for issuing registration certificates for vehicles as referred to in Directive 1999/37/EC, shall have access to the following data entered into the SIS II in accordance with Article 35 (2)(a)**,** (b) and (f) of that Decision for the sole purpose of checking whether vehicles presented to them for registration have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:

   (a) data concerning motor vehicles with a cylinder capacity exceeding 50cc (…);

   (b) data concerning trailers with an unladen weight exceeding 750 kg and caravans (…);

   (c) data concerning vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated.

   Subject to paragraph 2, the national law of each Member State shall govern access to that data by those services in that Member State.

2. Services referred to in paragraph 1 that are government services shall have the right to access directly the data entered in the SIS II.

3. Services referred to in paragraph 1 that are non-government services shall have access to data entered in the SIS II only through the intermediary of an authority referred to in Article 37 of that Decision. That authority shall have the right to access the data directly and to pass it on to the service. The Member State concerned shall ensure that the service and its employees are required to respect any limitations on the permissible use of data conveyed to them by the public authority.

4. Article 36 of Decision 2006/XX/JHA shall not apply to access made in accordance with this Article. The communication to the police or judicial

[34] OJ L 370, 17.12.2004, p.78
[35] OJ L 368, 15.12.2004 p. 26

authorities by services referred to in paragraph 1 of any information brought to light by access to the SIS II which gives rise to suspicion of a criminal offence shall be governed by national law.

Article 2

This Regulation replaces Article 102a of the Convention Implementing the Schengen Agreement.

Article 3

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from the date set in accordance with Article 65(1a) of Decision 2006/XX/JHA.

(1)

(2) This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

P6_TA-PROV(2006)0447

Establishment, operation and use of SIS II (decision) *

European Parliament legislative resolution on the proposal for a Council decision on the establishment, operation and use of the second generation Schengen information system (SIS II) (COM(2005)0230 – C6-0301/2005 – 2005/0103(CNS))

(Consultation procedure)

The European Parliament,

– having regard to the Commission proposal (COM(2005)0230)[36],

– having regard to Article 34(2)(c) of the Treaty on European Union,

– having regard to Article 39(1) of the Treaty on European Union, pursuant to which the Council consulted Parliament (C6-0301/2005),

– having regard to the Protocol integrating the Schengen acquis into the framework of the European Union, pursuant to which the Council consulted Parliament,

– having regard to Rules 93 and 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0353/2006),

1. Approves the Commission proposal as amended;

2. Calls on the Commission to alter its proposal accordingly, pursuant to Article 250(2) of the EC Treaty;

3. Calls on the Council to notify Parliament if it intends to depart from the text approved by Parliament;

4. Calls on the Council to consult Parliament if it intends to amend the Commission proposal substantially;

5. Instructs its President to forward its position to the Council and Commission.

[36] Not yet published in OJ.

PROPOSAL FOR A COUNCIL DECISION

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), Articles 31(1)(a) and (b) and Article 34(2)(c) thereof,

Having regard to the proposal from the Commission[37],

Having regard to the opinion of the European Parliament[38],

Whereas:

(1) The Schengen information system (hereinafter referred to as "SIS 1+") 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[39] (hereinafter referred to as the "Schengen Convention"), constitutes 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 the SIS (hereinafter referred to as "SIS II") has been entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[40] and Council Decision 2001/886/JHA[41] of 6 December 2001 on the development of the second generation Schengen Information System (SIS II). The SIS II will replace the SIS as established by the Schengen Convention.

(3) This Decision constitutes the necessary legislative basis for governing the SIS II in respect of matters falling within the scope of the Treaty on European Union (hereinafter referred to as the "EU Treaty"). Regulation (EC) No 2006/XX of the European Parliament and of the Council of the European Union on the establishment, operation and use of the SIS II[42] constitutes the

---

37 OJ C , , p. .

38 OJ C , , p. .

39 OJ L 239, 22.9.2000, p. 19. Convention as last amended by Council Decision 2005/211/JHA.

40 OJ L 328, 13.12.2001, p. 4.

41 OJ L 328, 13.12.2001, p. 1.

42 OJ L...

necessary legislative basis for governing the SIS II in respect of matters falling with the scope of the Treaty establishing the European Community (hereinafter referred to as the "EC Treaty").

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

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

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

(7) The expenditure involved in the operation of the Central SIS II and the Communication Infrastructure should be charged to the budget of the European Union.

(8) It is necessary to establish a manual setting out the detailed rules for the exchange of supplementary information in relation with the action required by the alert. 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 the Central SIS II and of parts of the Communication Infrastructure. However, in order to ensure a smooth transition between the SIS 1+ and the 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 permanent Management Authority with responsibility for these tasks should be established. The transitional period should last for no more than five years from the date of entry into force of this Decision.

(10) The SIS II should 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[43] should be processed in the SIS II.

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

(13) Alerts should not be kept longer in the SIS II than the time required to meet the purposes for which they were supplied. As a general principle, alerts on persons should be automatically erased from the 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 the SIS II after a period of ten years. The decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the review period and keep statistics about the number of alerts on persons the conservation period of which has been extended.

(14) (…)

(15) The SIS II should permit the processing of biometric data in order to assist in the reliable identification of individuals concerned. In the same context, the SIS II should also allow for the processing of data of 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.

(16) 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 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 (…) only be based on the grounds for refusal contained in that Framework Decision.

(16A) When a flag has been added in accordance with Article 14 C(2) 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.

---

[43] OJ L 190, 18.07.2002, p. 1.

(17) The SIS II should offer Member States the possibility to establish links between alerts. The establishment of links by a Member State between two or more alerts should have no impact on the action to be taken, the conservation period or the access rights to the alerts.

(18) Data processed in the SIS II in application of this Decision should not be transferred or made available to a third country or to an international organisation. 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 the 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. Article 9 of that 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 that Convention. The principles set out in the Convention should be supplemented or clarified in this Decision where necessary.

(20) The principles contained in Recommendation N° 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.

(20A) 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 co-operation in criminal matters, according to which it 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;

(21) 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[44] and in particular its Articles 21 and 22 as regards confidentiality and security of the processing applies to the processing of personal data by the Community institutions or bodies when carrying out their tasks as responsible for the operational management of the 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 the 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

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

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 2001/45 should be supplemented or clarified in this Decision where necessary.

(21A) 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 shall apply to officials or other servants of the European Communities employed and working in connection with SIS II.

(22) It is appropriate that National (…) Supervisory Authorities should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, appointed by 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[45], should monitor the activities of the Community institutions and bodies in relation to the processing of personal data taking into account the limited tasks of the Community institutions and bodies with regard to the data themselves.

(23) Liability of the Community arising from any breach by the Community institutions or bodies of this Decision is governed by the second paragraph of Article 288 of the EC Treaty.

(23A) Both Member States and the Commission should elaborate a security plan in order to facilitate the concrete implementation of security obligations and should cooperate with each other in order to address security issues from a common perspective.

(24) The provisions of the Convention of 26 July 1995 on the establishment of a European Police Office[46] (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 Article 24 of the Europol Convention, to monitor the activities of Europol and liability for any unlawful processing of personal data by Europol.

(25) The provisions of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime[47] concerning data protection apply to the processing of SIS II data by Eurojust, including the powers of the Joint Supervisory Body, set up under Article 23 of that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust.

(26) In order to ensure transparency, a report on the technical functioning of the Central SIS II and the Communication Infrastructure, including its security,

---

45 OJ L 12, 17.1.2004, p. 47.

46 OJ C 316, 27.11.1995, p. 2.

47 OJ L 63, 6.3.2002, p. 1.

and on the exchange of supplementary information should be produced every two years by the Management Authority. An overall evaluation should be issued by the Commission every four years.

(27) Certain aspects of the SIS II such as technical rules on entering, including data required for entering an alert, updating, deleting and searching, rules on compatibility and priority of alerts, the adding of flags, links between alerts and exchange of supplementary information cannot be covered exhaustively by the provisions of this Decision due to their technical nature, level of detail and need for regular update. (…) 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 will be decided to what extent the implementing measures could be a responsibility of the permanent Management Authority, as soon as it is set up.

(28) 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 XX/2006 should be the same.

(29) It is appropriate to lay down transitional provisions in respect of alerts issued in the SIS 1+ (…) which will be transferred to the 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 the SIS 1+ to the 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.

(30) It is necessary to lay down special provisions regarding the remainder of the budget affected to the operations of the SIS which are not part of the budget of the European Union.

(31) 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.

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

(33) 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[48].

(34) 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[49].

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

(36) 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 which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC of 17 May 1999[50] on certain arrangements for the application of that Agreement[51].

(36A) An arrangement has to 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[52], annexed to the abovementioned Agreement.

(37) As regards Switzerland, this Decision constitutes a development of the 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 Council Decision 1999/437/EC read in conjunction with Article 4(1) of the Council decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement[53].

---

48 OJ L 131, 1.6.2000, p. 43.
49 OJ L 64, 7.3.2002, p. 20.
50 OJ L 176, 10.7.1999, p. 6.
51 OJ L 176, 10.7.1999, p. 31
52 OJ L 176, 10.7.1999, p. 53.
53 OJ L 368, 15.12.2004, p. 26

(37A) An arrangement has to 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.

(38) 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.

(39) This Decision should apply to the States concerned by Recitals 33, 34, 37 and 38 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 objective of the SIS II

1. The second generation Schengen Information System (hereinafter referred to as "SIS II") is hereby established.

2. The purpose of the SIS II shall be, in accordance with this Decision, to ensure a high level of security within an area of freedom, security and justice, (…) 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 the Treaty establishing the European Community (hereinafter referred to as "EC Treaty") relating to the movement of persons in their territories, using information communicated via this system.

Article 2
Scope

1. This Decision defines the conditions and procedures for the processing of alerts on persons and objects in the SIS II and 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 in particular on the technical architecture of the SIS II, the responsibilities of the Member States and of the Management Authority referred to in Article 12, 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 the SIS II allowing the competent authorities to identify a person or an object in view of a specific action to be taken;

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

   - in order to allow Member States to consult or inform each other whilst entering an alert;

   - a hit in order to allow the appropriate action to be taken;

   - when the required action cannot be taken;

   - when dealing with the quality of SIS II data;

   - when dealing with the compatibility and priority of alerts;

   - when dealing with the exercise of the right of access;

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

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

2. *(…)*

2a Any reference in this Decision to provisions of the Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third states on the basis of Articles 24 and 38 of the Treaty on European Union 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. The SIS II is composed of:

(aa) a central system (hereinafter referred to as “the Central SIS II”) composed of:

– a technical support function (hereinafter referred to as “CS-SIS”) containing the (…) SIS II database;

– a uniform national interface (hereinafter referred to as “NI-SIS”);

(a) anational section (hereinafter referred to as “N.SIS II") in each of the Member States, consisting of the national data systems which communicate with the Central SIS II. An N.SIS II may contain a data file (hereinafter referred to as “national copy”), containing a complete or partial copy of the SIS II database;

(b) *(moved to (aa))*

(c) a communication infrastructure between the CS-SIS and the NI-SIS (hereinafter referred to as "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 N.SIS II. 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. The principal CS-SIS, which carries out technical supervision and administration, is located in Strasbourg (France) and a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in case of failure of this system, is located in Sankt Johann im Pongau (Austria).

4. The CS-SIS will provide the services necessary for the update of, and the searches in, the SIS II (…) database. For the Member States which use a national copy the CS-SIS will provide:

- the on-line update of the national copies;

- the synchronisation and the coherence between the national copies and the (…) SIS II database;

- the operation for initialisation and restoration of the national copies.

Article 5
Costs

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

2. These costs will include work done with respect to the 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.

4. *(…)*

CHAPTER II
Responsibilities of the Member States

Article 6
National Systems

Each Member State (…) shall be responsible for:

(a) setting up, operating and maintaining its N.SIS II;

(b) connecting its N.SIS II to the NI-SIS.

Article 7
N.SIS II Office and SIRENE Bureau

1. (a) Each Member State shall designate an authority (hereinafter referred to as "N.SIS I Office"), which shall have central responsibility for its N.SIS II;

   (b) The said 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.

   (c) Each Member State shall transmit its alerts via the N.SIS II Office.

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

(b) This Bureau shall also coordinate the verification of the quality of the information entered into the SIS II (…).

(c) For those purposes it shall have access to data processed in the SIS II.

3. The Member States shall inform the Management Authority referred to in Article 12 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 40(7).

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.

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

3. Should the Communication Infrastructure be unavailable, Member States may use other adequately secured technical means for exchanging supplementary information.

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

3a Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 in the form of a manual called the "SIRENE Manual", without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

Article 9
Technical compliance

1. To ensure the rapid 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 the CS-SIS with the N-SIS II. These protocols and technical procedures shall be established in accordance with the procedure referred to in Article 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

2. If a Member State uses a national copy it shall ensure, by means of the services provided by the CS-SIS (…) that data stored in the national copy is, through automatic updates referred to in Article 4(4), identical and consistent

with the SIS II database, and (…) that a search in its national copy will provide an equivalent result as a search in the SIS II database.

Article 10
Security (…)

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

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

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

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

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

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

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

(ea) 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 for persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities without delay upon their request (personnel profiles)

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

(g) 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);

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

(ha) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure the 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.

3. *(…)*

4. (…)

Article 10 A
Confidentiality

Each Member State shall apply its rules of professional secrecy or other equivalent obligations 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 11
Keeping of records at national level

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

(b) 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(a), with the exception of exchanges connected to the services referred to in Article 4(4).

1a *(moved to 1(b))*

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 a search, the reference to the data transmitted and the name of both the competent authority and the person responsible for processing the data.

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

4. Records may be kept longer if they are required for monitoring procedures which have already begun.

4a The competent national authorities in charge of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning of the N.SIS II, data integrity and security, shall have access, within the limits of their competence and upon request, to these records to ensure that they are able to fulfil their tasks.

Article 11 A
Self-monitoring

The Member States shall ensure that each authority entitled to access SIS II data shall take the measures necessary to ensure compliance with this Decision and shall cooperate, with the National Supervisory Authority, as referred to in Article 53.

Article 11 B
Staff training

Before being authorised to process data stored in the SIS II, staff of the authorities with a right to access the 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 12
Operational management

1. A Management Authority, which shall be funded by the budget of the European Union, shall be responsible for the operational management of the Central SIS II. It shall also be responsible for the following tasks related to the Communication Infrastructure:

   (a) supervision;

   (b) security;

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

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

(a) budget implementing tasks;

(b) acquisition and renewal;

(c) contractual matters.

3. During a transitional period before the Management Authority mentioned in paragraph 1 takes up its responsibilities, the Commission shall be responsible for the operational management of the Central SIS II. The Commission may entrust the exercise of this management as well as of budget implementing tasks, 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[54], to national public sector bodies, in two different countries.

3aa Each national public sector body, as referred to in paragraph 3, must comply in particular with the following selection criteria:

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

(b) it must possess a long term expertise in the service and security requirements of an information system comparable to the functionalities 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 provided for in Article 4;

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

(e) it must work in an administrative environment allowing it to implement its tasks properly and avoid any conflict of interests.

3a The Commission shall prior to any such delegation and at regular intervals afterwards inform the European Parliament and the Council about the conditions of delegation, the precise scope of the delegation, and the bodies to which tasks are delegated.

3b In case the Commission delegates its responsibility during the transitional period pursuant to paragraph 3 it shall ensure that this delegation fully respects the limits set by the institutional system laid out in the Treaty. It shall ensure, in particular, that this delegation does not adversely affect any effective control mechanism under European Union law, be it by the Court of Justice, the Court of Auditors or the European Data Protection Supervisor.

---

[54] OJ L 248, 16.09.2002, p. 1-48.

4. Operational management of the Central SIS II shall consist of all the tasks necessary to keep the Central SIS II functioning on a 24 hours a day, 7 days a week basis in accordance with this Decision, in particular the maintenance work and technical developments necessary for the smooth running of the system.

5. *(deleted)*

6. 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 the Central SIS II.

Article 13
Security (…)

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

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

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

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

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

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

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

(ea) 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 without delay upon its request (personnel profiles);

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

(fa) 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);

(g) 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);

(ga) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure the 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.

3. (…)

Article 13 A
Confidentiality

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 obligations of confidentiality to all its staff required to work with SIS II data on comparable standards to those provided in Article 10 A. 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 14
Keeping of records at central level

1. The Management Authority shall ensure that every access to and all exchanges of personal data within the CS-SIS are recorded for the purposes provided for in Article 11(1).

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 a search, the reference to the data transmitted and the identification of the competent authority responsible for processing the data.

3. The records may only be used for the purposes provided for in paragraph 1 and shall be deleted at the earliest after a period of one year and at the latest after a

period of three years after their creation. The records which include the history of alerts shall be erased after a period of one to three years after the deletion of the alerts.

4. Records may be kept longer if they are required for monitoring procedures which have already begun.

4a The competent authorities in charge of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning of the CS-SIS, data integrity and security, shall have access, within the limits of their competence and upon request, to these records to ensure that they are able to fulfil their tasks.

Article 14 AA
Information campaign

The Commission shall, in co-operation with the National Supervisory Authorities referred to in Article 53(1a), and the European Data Protection Supervisor, referred to in Article 53 A(1), accompany the start of the operation of the SIS II with an information campaign informing the public about the objectives, the data stored, the authorities with access and the rights of persons. After its establishment, the Management Authority, in co-operation 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 in general about the SIS II.

Chapter III A
Categories of data and Flagging

Article 14 A
Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Decision providing for the storage of additional data, the 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 15, 23, 27, 31 and 35.

2. The categories of data shall be as follows:

   (a) persons for whom an alert has been issued;

   (b) objects referred to in Articles 31 and 35.

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

(a) surname(s) and forename(s), name at birth and previously used names and any aliases possibly 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 persons concerned are armed, violent or have 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 the SIS II pursuant to Article 46;

(n) the type of offence.

4. *(…)*

5. 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 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

5a The technical rules necessary for searching data referred to in paragraph 5 shall be similar for searches in the CS-SIS, in national copies and in technical copies, as referred to in Article 40(2).

Article 14 AB
Proportionality clause

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

Article 14 AC
Specific rules for photographs and fingerprints

Photographs and fingerprints as referred to in Article 14 A(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 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

(b) Photographs and fingerprints shall only be used to confirm the identity of a person who has been found as a result of an alphanumeric search made in the SIS II.

(c) As soon as technically possible, fingerprints may also be used to identify a person on the basis of his/her biometric identifier. Before this functionality is implemented in the 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 14 AD
Requirement for an alert to be entered

1. Alerts on persons cannot be entered without the data referred to in Articles 14 A(3)(a), 14 A(3)(d), 14 A(3)(l) as well as, where applicable, Article 14 A(3)(k).
2. In addition, when available, all other data listed in Article 14 A(3) shall (…) be entered.

Article 14 B
General Provisions on Flagging

1. Where a Member State considers that giving effect to an alert entered in accordance with Article 15, Article 23 or Article 31 is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag is 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 15, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.

3. *(…)*

4. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the executing Member State shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State 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 14 C
Flagging related to alerts for arrest for surrender purposes

1. Where Framework Decision 2002/584/JHA[55] 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 IV
Alerts in respect of persons wanted for arrest for surrender or extradition purposes

Article 15
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 states on the basis of Articles 24 and 38 of the Treaty on European Union 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 16
Additional data on persons wanted for arrest with a view to surrender or extradition (…)

[55] OJ L 190, 18.07.2002, p. 1.

Article 17
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 into the 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 17 A
Supplementary information on persons wanted for arrest for surrender purposes

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

Article 17 B
Supplementary information on persons wanted for arrest for extradition purposes

1. The Member State which entered the alert into the SIS II for extradition purposes shall communicate the following data 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 judgement;

   (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) or 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 17 or 17 A has already been provided and is considered being sufficient for the execution of the alert by the executing Member State.

Article 18
Authorities with right to access to alerts and additional data on persons wanted for arrest

(…)

Article 19
Conservation period of the alerts and additional data for arrest

(…)

Article 20
Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes

If the arrest cannot be made either because (…) a requested Member State refuses in accordance with the procedures on flagging set out in Articles 14 B or 14 C, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, this Member State must regard the alert as being an alert for the purposes of communicating the whereabouts of the person concerned.

Article 21
Flagging related to alerts for arrest and surrender

(…)

Article 22
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 the SIS II in accordance with Article 15 in combination with the additional data referred to in Article 17, 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 the SIS II (…) in accordance with Article 15 and 17 B shall have the same 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, as amended by the protocol of 11 May 1974.

Chapter V
Alerts on missing persons (…)

Article 23
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 into the 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.

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

2b Paragraphs 1 to 2a shall apply in particular to minors.

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

Article 24
Authorities with right to access to alerts

(…)

Article 25
Conservation period of the alerts

(…)

Article 26
Execution of action based on an alert

1. Where persons referred to in Article 23 are found, the competent authorities shall, subject to paragraph 2, communicate their whereabouts to the Member State issuing the alert. They may, in the cases referred to in Article 23(2)(a) move the persons to a safe place in order to prevent them from continuing their 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 found 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 an interested person who reported the person missing.

Chapter VI
Alerts on persons who are sought so as to be able to assist with a judicial procedure

Article 27
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 the SIS II data on:

– witnesses;

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

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

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

Article 28
Authorities with right to access to alerts

(…)

Article 29
Conservation period of alerts

(…)

Article 30
Execution of the action based on an alert

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

Chapter VII
Alerts on persons and objects for discreet checks or specific checks

Article 31
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 of specific checks in accordance with Article 32(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 an(…) serious criminal offence, such as the offences (b) 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(d) , 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 32(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.

3a 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 32
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 may be collected and communicated to the authority issuing the alert when border control or other police and customs checks are carried out within the country:

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

   (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 found.

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 the specific checks referred to in Article 31, persons, vehicles, boats, aircraft, containers and objects carried may be searched in accordance with national law for the purposes referred to in that Article. 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.

Article 33
Authorities with right to access to alerts

(…)

Article 34
Conservation period of alerts

(…)

Chapter VIII
Alerts on objects for seizure or use as evidence in criminal proceedings

Article 35
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 the 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 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

Article 36
Execution of the action based on an alert

1. If a search brings to light an alert for an object which has been found, 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 measures to be taken by the Member State which found the object must be in accordance with its national law.

Chapter VIII A
Right to access and conservation of alerts

Article 37
Authorities with the right to access alerts

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

(a) border control, in accordance with Regulation 562/2006/EC 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);

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

2. However, access to data entered in the SIS II and the right to search such data directly may also be exercised by national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation, as well as their co-ordinating authorities.

3. *(moved to Article 37 C)*

3a The authorities referred to in this Article shall be included in the list referred to in Article 40(7).

Article 37 A
Access to SIS II data by Europol

1. The European Police Office(Europol) shall within its mandate have the right to have access to, and to search directly, data entered into the SIS II in accordance with Articles 15,(…), 31 and 35.

2. *(moved to Article 37 C)*

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

4. 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 States and third bodies with the consent of the Member State concerned.

5. Europol may request further information from the Member State concerned in accordance with the provisions set out in the Europol Convention.

6. Europol shall:

(a) record every access and search made by it, in accordance with the provisions of Article 11;

(b) without prejudice to paragraphs 4 and 5, not connect parts of the SIS II nor transfer the data contained therein to which it has access to any computer system for data collection and processing in operation by or at Europol nor download or otherwise copy any parts of the SIS II;

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

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

(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 accede to and to search data entered into the SIS II.

Article 37 B
Access to SIS II data by Eurojust

1. The national members of Eurojust and their assistants shall within their mandate have the right to have access to, and search, data entered in accordance with Articles 15, 23, 27 and 35 into the SIS II.

2. *(moved to Article 37 C)*

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

4. Nothing in this article shall be interpreted as affecting the provisions of the Council Decision setting up Eurojust 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 Article 23 of that Council Decision.

5. Every access and search made by a national member of Eurojust or an assistant shall be recorded in accordance with the provisions of Article 11 and every use made by them of data to which they have acceded shall be registered.

6. No parts of the 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 in operation by or at Eurojust nor shall any parts of the SIS II be downloaded.

7. The access to data entered into the SIS II shall be limited to the national members and their assistants and not be extended to Eurojust staff.

8. Measures as provided for in Articles 10 and 10 A shall be adopted and applied.

Article 37 C
Limits of access

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

Article 38
Conservation period of alerts on persons

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

2. Within three years of entering such an alert into the SIS II the necessity of keeping the alert shall be reviewed by the Member State issuing it. The period shall be one year in the case of alerts on persons pursuant to Article 31.(…)

2aa Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

2a The Member State issuing the alert may, within the review period, decide, following a comprehensive individual assessment, which shall be(…) recorded, to keep the alert should this prove necessary for the purposes for which the alert was issued. In this case paragraph 2 applies accordingly. Any extension of the alert must be communicated to the CS-SIS.

3. Alerts shall automatically be erased after the reviewing period referred to in paragraph 2 has expired. This will not apply in case the Member State issuing the alert communicated the extension of the alert to the CS-SIS as referred to in paragraph 2a. The CS-SIS shall automatically inform the Member States of scheduled deletion of data from the system four months in advance.

4. *(moved to paragraph 3)*

4a Member States shall keep statistics about the number of alerts the conservation period of which has been extended in accordance with paragraph 2a.

5. *(…)*

6. *(…)*

Article 38 A
Conservation period of alerts on objects

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

2. Alerts on objects entered in accordance with Article 31 shall be kept for a maximum of five years.

3. Alerts on objects entered in accordance with Article 35 shall be kept for a maximum of ten years.

4. The conservation 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 this case, paragraphs 2 and 3 apply accordingly.

CHAPTER IX
General data processing rules

Article 39
Categories of data

(…)

Article 40
Processing of SIS II data

1. The Member States may process the data provided for in Articles 15, 23, 27, 31 and 35 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 37 to carry out a direct search. The provisions of this Decision shall apply to these copies. Alerts issued by other Member States may not be copied from the N.SIS II into other national data files.

2A (a) Technical copies, as referred to in paragraph 2, which lead to off-line databases may only be created for a period that shall not exceed 48 hours. This duration may be extended in emergency situations. These copies shall be destroyed once the emergency situation comes to an end.

(b) (...) Member States shall keep an up-to-date inventory of these copies, make this inventory available to National Supervisory Authorities, as referred to in Article 53(1a) and ensure that the provisions of this Decision, in particular those referred to in Article 10, are applied in respect of these copies.

3. Access to SIS II data shall only be authorised within the limits of the competence of the national authority and to duly authorised staff.

4. With regard to the alerts laid down in Articles 15, 23, 27, 31 and 35 of this Decision, any processing of information contained therein for purposes other than those for which it was entered into the 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.

5. Data may not be used for administrative purposes.

6. Any use of data which does not comply with paragraphs 1 to 5 shall be considered as misuse under the national law of each Member State.

7. Each Member State shall send to the Management Authority a list of competent authorities which are authorised to search the data contained in the SIS II directly pursuant to this Decision and any changes thereto. That 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.

Article 41
Entering a reference number

(…)

Article 42
SIS II data and national files

1. Article 40(2) shall not prejudice the right of a Member State to keep in its national file 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 40(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert, which that Member State has issued in the SIS II.

Article 42 A
SIS II alerts and national law

1. *(…)*

2. Insofar 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.

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

Article 43
Quality of the data processed in the SIS II(…)

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

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

3. If one of the Member States which has not issued the 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 issuing the alert thereof at the earliest opportunity and not later than ten days after the said evidence has come to its attention; the latter 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 case to the European Data Protection Supervisor who shall jointly with the involved National Supervisory Authorities, as referred to in Article 53(1a), act as mediator.

5. *(…)*

5a The Member States shall exchange supplementary information if a person claims not to be the person wanted by an alert. If the outcome of the check is that there are in fact two different persons this person shall be informed about the provisions referred to in Article 44.

6. Where a person is already the subject of an alert in the 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 43 A
Distinguishing between persons with similar characteristics

When, while introducing a new alert, it appears that there is already a person in the SIS II with the same identity description element, the following procedure shall be followed:

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

(b) if the cross-check reveals that the person in question is indeed one and the same, the SIRENE bureau shall apply the procedure for entering multiple alerts as referred to in Article 43(6). If the outcome of the check is that there are in fact two different people, the SIRENE bureau approves the request for entering another alert by adding the necessary elements to avoid any misidentifications.

Article 44
Additional data for the purpose of dealing with misused identities

1. Where confusion may arise between the person actually intended by 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 related to the latter to the alert in order to avoid the negative consequences of misidentifications.

2. The data related to a person whose identity has been misused shall only be (…) used for the following purposes:

   (a) to allow the competent authority to differentiate the person whose identity has been misused from the person actually intended by 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. No more than the following personal data may be entered and further processed in SIS II for the purpose of this article:

   (a) surname(s) and forename(s), name 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 issuing.

3a The technical rules necessary for entering, updating and deleting the data referred to in paragraph 3 shall be established in accordance with the procedure referred to in Article 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

4. 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.

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

Article 45
Flagging

(…)

Article 46
Links between alerts

1. A Member State may create a link between alerts it issues in the 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 conservation period of each of the linked alerts.

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

3a A Member State shall create a link between alerts only when there is a clear operational need.

3b 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.

4. When a Member State considers that the creation of a link by another Member State 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.

4a The technical rules for linking alerts shall be adopted in accordance with the procedure defined in Article 61, without prejudice to the provisions of the instrument setting up the Management Authority referred to in Article 12.

Article 47
Purpose and conservation period of supplementary information

1. Member States shall keep a reference to the decisions giving rise to the 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 alert related to the person concerned has been deleted from the 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 of time for which such data may be held in such files shall be governed by national law.

Article 48
Transfer of personal data to third parties

1. (…) Data processed in the SIS II in application of this Decision shall not be transferred or made available to a third country or to an international organisation.

2. *(…)*

Article 48 AA
Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol

1. By way of derogation from Article 48, the passport number, country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered into the SIS II may be exchanged with members of Interpol by establishing a connection between the 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 the 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 the SIS II.

CHAPTER X
Data protection

Article 48 A
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 not be authorised.

Article 49
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 50
Right of access, correction of inaccurate data and deletion of unlawfully stored data

1. The right of persons to have access to data entered in the SIS II in accordance with this Decision which relate to them shall be exercised in accordance with the law of the Member State before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 53(1) shall decide whether information shall be communicated and by what procedures. A Member State which has not issued the alert may communicate information concerning such data only if it has previously given the Member State issuing the alert an opportunity to state its position. This shall be done through the exchange of supplementary information.

2. Communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties.

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

3a 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. If national law provides for a shorter delay, the latter shall be respected.

3b 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 3 months from the date on which he applies for correction or deletion. If national law provides for a shorter delay, the latter shall be respected.

Article 51
Right of access, rectification and erasure

(…)

Article 52
Remedies

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

2. The Member States undertake mutually to enforce final decisions taken by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 54.

3. The rules on remedies provided for in this Article shall be evaluated by the Commission two years after the entry into force of this Decision.

Article 53
Supervision of the N.SIS II

1a Each Member State shall ensure that an independent authority (hereinafter referred to as the "National Supervisory Authority") monitors independently the lawfulness of the processing of SIS II personal data on and from their territory, including the exchange and further processing of supplementary information.

1b The authority or authorities referred to in paragraph 1a shall ensure that at least every four years an audit of the data processing operations in the N.SIS II is carried out according to international auditing standards.

1c Member States shall ensure that the authority or authorities referred to in paragraph 1a have sufficient resources to fulfil the tasks entrusted to them by this Decision.

2. (…)

3. *(…)*

4. *(…)*

5. *(…)*

6. *(…)*

Article 53 A
Supervision of the Management Authority

1. The European Data Protection Supervisor shall monitor the personal data processing activities of the Management Authority. The duties and powers referred to in Articles 46 and 47 of 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 shall apply accordingly.

2. The European Data Protection Supervisor shall ensure that at least every four years an audit of the Management Authority's personal data processing activities is carried out according to international auditing standards. The report of the 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 53 B
Cooperation between National Supervisory Authorities and the EDPS

1. The National Supervisory Authorities (…) and the European Data Protection Supervisor, each acting within the scope of their 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 their 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 the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as may be needed.

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 at the charge of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly according to need. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years.

Article 53 C
Data protection during the transitional period

In case the Commission delegates its responsibilities during the transitional period, pursuant to Article 12(3), it shall ensure that the European Data Protection Supervisor shall have the right and possibility to fully exercise his tasks including the possibility to carry out checks on the spot or to exercise (…) any other powers endowed to the European Data Protection Supervisor by Article 47 of 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.

CHAPTER XI
Liability and sanctions

Article 54
Liability

1. Each Member State shall be liable in accordance with its national law for any injury caused to a person through the use of the N.SIS II. This shall also apply to injury 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 data were used by the Member State requesting reimbursement in breach of this Decision.

3. If failure of a Member State to comply with its obligations under this Decision causes damage to the SIS II, that Member State shall be held liable for such damage, unless and insofar as the Management Authority or other Member State(s) participating in the SIS II failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

Article 55
Sanctions

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

CHAPTER XII
Access to SIS II by Europol and Eurojust

(…)

CHAPTER XIII
Final Provisions

Article 59
Monitoring and statistics

1. The Management Authority shall ensure that procedures are in place to monitor the functioning of the SIS II against objectives, in terms of 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 related to the processing operations performed in the Central SIS II.

2a 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 the SIS II was accessed, respectively given as a total and for each Member State.

3. Two years after the SIS II starts operations and every two years thereafter, the Management Authority shall submit to the European Parliament and the Council a report on the technical functioning of the Central SIS II and the Communication Infrastructure, including its security, the bilateral and multilateral exchange of supplementary information between Member States.

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

5. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraph 2a, 3 and 4.

5a. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 4.

(…)

Article 60
Advisory Committee

(…)

Article 61
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 reexamine 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 the date of entry into force of this Decision.

Article 62
Amendment of the provisions of the Schengen Acquis

1. For the purposes of matters falling within the scope of the EU Treaty, this Decision replaces on the date referred to in Article 65(1a) 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 also repeals, on the date referred to in Article 65(1a), the following provisions of the Schengen acquis implementing those articles[56]:

   – 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);

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

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

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

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

– 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);

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

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

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

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

– 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 and shall be read in accordance with the correlation table set out in the Annex.

Article 63
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 65(1a).

Article 64
Transitional period and budget

1. Alerts may be transferred from SIS 1+ to the SIS II. The Member States shall ensure, giving priority to the alerts on persons, that the contents of the alerts that are transferred from the SIS 1+ to the SIS II satisfy the provisions of this Decision (…) as soon as possible and within three years of the date referred to in Article 65(1a) at the latest. During this transitional period, the Member States may continue to apply the provisions of Articles 94, 95, 97, 98, 99, 100 (…) of the Schengen Convention to the contents of the alerts that are transferred from the SIS 1+ to the SIS II subject to the following rules:

– (…) in the event of a modification of, an addition to or a correction or update (…) of the content of an alert transferred from the SIS 1+ to the 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;

– in the event of a hit on an alert transferred from the SIS 1+ to the 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.

1a (…)

2. The remainder of the budget at the date set in accordance with Article 65(1a), 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 12(3), references in this Decision to the Management Authority shall be construed as a reference to the Commission.

Article 65
Entry into force, applicability and migration

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

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

2. The date referred to in paragraph 1a shall be fixed after:

(a) the necessary implementing measures have been adopted;

(b) all Member States fully participating in the 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 the 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. This validation will confirm that the level of performance of the SIS II is at least equivalent to that achieved with SIS 1+;

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

2a The Commission shall inform the European Parliament of the results of the tests carried out according to paragraph 2(c).

3. Any Decision of the Council taken in accordance with paragraph 1 shall be published in the *Official Journal of the European Union*.

4. (deleted)

Done at Strasbourg,

For the Council
The *President*

ANNEX
Correlation table

Schengen Convention[57] Articles	**Decision Articles**
Art. 92(1)	Art. 1(1); Art. 2(1); Art. 4(1)(2)(3)
Art. 92(2)	Art.4 (1) (2) (3); Art. 5(2 Art. 6; Art.9
Art. 92(3)	Art.4 (1)(2)(3); Art.5(1); Art
Art. 92(4)	Art.3 (1); Art. 7(2)(3); Art.8
Art. 93	Art.1(2)
Art. 94(1)	Art. 40(1)
Art. 94(2)	Art.15; Art.23 (1) ; Art.27 ; 31(1) Art. 35(1)
Art. 94(3)	Art. 39(1); Art. 44(3)
Art. 94(4)	Art. 45
Art. 95(1)	Art. 15
Art. 95(2)	Art. 16; Art. 17; Art. 45
Art. 95(3)	Art.20; Art. 21; Art. 45
Art. 95(4)	Art. 45(5)
Art. 95(5)	Art. 20(1)
Art. 95(6)	Art. 22
Art. 96(1)	
Art. 96(2)	
Art. 96(3)	
Art. 97	Art. 23; Art. 26
Art. 98(1)	Art. 27

[57] Articles and paragraphs in italics have been added or amended by Council Regulation (EC) No. 871/2004 and Council Decision 2005/211/JAI on the introduction of new functions for the Schengen Information System, including the fight against terrorism

Schengen Convention[57] Articles	**Decision Articles**
Art. 98(2)	Art. 30
Art. 99(1)	Art. 31(1)
Art. 99(2)	Art. 31(1)
Art. 99(3)	Art. 31(2)
Art. 99(4)	Art. 32(1)(2)(3)
Art. 99(5)	Art. 32(4)
Art. 99(6)	Art. 45
Art. 100(1)	Art. 35
Art. 100(2)	Art. 36
Art. 100(3)	Art. 35
Art. 101(1)	Art. 18(1)(4); Art. 24; Art. 28(1)(2); Art.33(1)(2); 37(1)(2)
Art. 101(2)	
Art. 101(3)	Art. 40(3)
Art. 101(4)	Art. 40(4)
Art. 101A(1)	Art. 18(2); Art. 33(3); Art. 3
Art. 101A(2)	Art. 18(2); Art. 33(3); Art. 3
Art. 101A(3)	Art. 57(1)
Art. 101A(4)	Art. 57(2)
Art. 101A(5)	Art. 57(7)
Art. 101A(6)	Art. 53(2); Art. 57(4)(5)(6)
Art. 101B(1)	Art. 18(3); Art. 28(3)
Art. 101B(2)	Art. 18(3); Art. 28(3); Art. 58(8)
Art. 101B(3)	Art. 58(1)(2)

Schengen Convention[57] Articles	Decision Articles
Art. 101B(4)	Art. 53(2); Art. 58(3)
Art. 101B(5)	Art. 58(5)
Art. 101B(6)	Art. 58(6)
Art. 101B(7)	Art. 58(8)
Art. 101B(8)	Art. 58(4)
Art. 102(1)	Art. 40(1)
Art. 102(2)	Art. 42(1)(2)
Art. 102(3)	Art. 40(2)
Art. 102(4)	
Art. 102(5)	Art. 54(1)
Art. 103	Art. 11
Art. 104(1)	
Art. 104(2)	
Art. 104(3)	
Art. 105	Art. 43(1)
Art. 106(1)	Art. 43(2)
Art. 106(2)	Art. 43(3)
Art. 106(3)	Art. 43(4)
Art. 107	Art. 43(6)
Art. 108(1)	Art. 7(1)
Art. 108(2)	
Art. 108(3)	Art. 6; Art. 7(1); Art. 9(1)
Art. 108(4)	Art. 7(3)
Art. 109(1)	Art. 50(1); Art. 51(1)(2)(3)

Schengen Convention[57] Articles	Decision Articles
Art. 109(2)	Art. 51(4)
Art. 110	Art. 51(1)(5); Art.53(1)
Art. 111(1)	Art. 52
Art. 111(2)	
Art. 112(1)	Art. 19(1)(2); Art.25(1)(2); Art. 29(1)(2); Art.34(1)(2 Art. 43(7)
Art. 112(2)	Art. 43(7)
Art. 112(3)	Art. 19(3); Art. 25(3); Art. 29(3); Art. 34(4); Art. 38(5)
Art. 112(4)	Art. 19(2); Art. 25(2); Art. 29(2); Art. 34(3); Art. 38(4)
Art. 112A(1)	Art. 47(1)
Art. 112A(2)	Art. 47(2)
Art. 113(1)	Art. 38(1)(2)(3)
Art. 113(2)	Art. 14(3)(4)(5)(6)
Art. 113A(1)	Art. 47(1)
Art. 113A(2)	Art. 47(2)
Art. 114(1)	Art. 53(1)
Art. 114(2)	Art. 53
Art. 115(1)	Art. 53(3)
Art. 115(2)	
Art. 115(3)	
Art. 115(4)	
Art. 116(1)	Art. 54(1)

Schengen Convention[57] Articles	Decision Articles
Art. 116(2)	Art. 54(2)
Art. 117(1)	Art. 49
Art. 117(2)	
Art. 118(1)	Art. 10(1)
Art. 118(2)	Art. 10(1)
Art. 118(3)	Art. 10(3)
Art. 118(4)	Art. 13
Art. 119(1)	Art. 5(1); Art. 64(2)
Art. 119(2)	Art. 5(2)(3)