COUNCIL OF THE EUROPEAN UNION

Brussels, 24 March 2006

5709/1/06 REV 1

LIMITE

SIRIS 22
SCHENGEN 10
CODEC 71
COMIX 86

Interinstitutional File: 2005/0106 (COD)

NOTE

from :	Presidency
to :	Schengen Acquis Working Party (Mixed Committee EU/Iceland, Norway and Switzerland)
No. prev. doc. :	9943/05 SIRIS 61 SCHENGEN 11 CODEC 486 COMIX 384 11760/05 SIRIS 81 SCHENGEN 23 COMIX 534 13134/05 SIRIS 101 SCHENGEN 31 COMIX 652 14498/1/01 SIRIS 125 SCHENGEN 41 COMIX 768 REV 1
Subject :	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) - Redrafted proposal

Following discussions in the Schengen Acquis Working Party since July 2005, and taking into account the preparatory proceedings of the LIBE Committee of the European Parliament as well as the delegations' comments, the Austrian Presidency presents in the Annex a redrafted compromise version of the abovementioned proposal.

DRAFT COUNCIL REGULATION 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 Article 62 (2)(a), 63 (3)(b) and Article 66 thereof,

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 Regulation, to maintain public policy and a high level of public security, including national 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")[1] relating to the movement of persons in their territories, using information communicated via this system.

Article 2

Scope

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

[1] DK requested the insertion of a recital identical to Recital 9 of Council Regulation (EC) No. 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism.

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

Article 3

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 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, following a hit in order to allow the appropriate action to be taken, when the required action cannot be taken, when dealing with the quality of SIS II data and when dealing with the compatibility of alerts as well as 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;[2]
   (d) "third country national" means any individual who is not a citizen of the European Union within the meaning of Article 17 (1) of the EC Treaty.
2. "Processing of personal data", "processing", and "personal data" shall be understood in accordance with Article 2 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[3].[4]

---

[2] As a result of the deletion of the reference to beneficiaries of the Community right of free movement, delegations are invited to consider the status of Declaration of the Executive Committee of 18 April 1996 defining the concept of an alien (SCH/COM-Ex (96) decl 5).

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

[4] The application of Directive 95/46/EC as the *lex generalis* on data protection does not prevent the SIS II Regulation from limiting some of the rights contained therein such as the right of information foreseen by Article 11 (1) of this Directive.

[5]Article 4

Technical architecture and ways of operating the SIS II

1. The SIS II is composed of:
   (a) a national section (hereinafter referred to as "N.SIS II") in each of the Member States;
   (b) 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 reference database for SIS II;
      – a uniform national interface (hereinafter referred to as "NI-SIS")[6];
   (c) a communication infrastructure between the CS-SIS and the NI-SIS (hereinafter referred to as "Communication Infrastructure").
2. SIS II data shall be searched via the N.SIS II. A N.SIS II may contain a data file (hereinafter referred to as "national copy"), containing a complete or partial copy from the reference database for SIS II. A national copy shall be available for the purposes of carrying out automated searches in the territory of each of the Member States.
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 in Pongau (Austria).
4. The CS-SIS will provide the services necessary for the update of, and searches in, the reference database for SIS II. 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 reference database for SIS II;
   – the operation for initialisation and restoration of the national copies.

---

5 Scrutiny reservations by DE and SI.

6 DE and IT asked for the legal instrument to foresee the possibility of choosing one or two access points.

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 synchronisation and the coherence between the national copies and the reference database for SIS II, including the operation for initialisation and restoration of the national copies.
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, for its own account and at its own risk, shall:

(a) set up, operate and maintain its N.SIS II;

(b) connect 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 II office"), which shall have central responsibility for its N.SIS II;

   (b) The said authority shall be responsible for the smooth operation of the N.SIS II, shall ensure the access of the competent authorities to the SIS 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[7];

   (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 referred to in Article 12 shall publish the list of them together with the list referred to in Article 21 (3).

---

[7] The procedure for the development and adoption of the SIRENE Manual will be the object of a separate discussion concerning the implementing measures.

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual[8] 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 technical means for exchanging supplementary information.

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 procedures established for that purpose.
2. If a Member State uses a national copy it shall, by means of the services provided by CS-SIS, ensure that its national copy will provide an equivalent result as a search in the central database.

Article 10

Security and confidentiality

1. Each Member State shall, in relation to its N.SIS II, adopt the necessary measures 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 equipment used for processing personal data (equipment 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);

[8] The procedure for the development and adoption of the SIRENE Manual will be the object of a separate discussion concerning the implementing measures.

(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 only have access to the data covered by their access authorisation and with individual and unique user identities and confidential passwords only (data access control);

(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 appropriate encryption techniques (transport control).

2. (…)

3. Each Member State shall apply his 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, according to his 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. Each Member State 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-auditing, ensuring the proper functioning of the N.SIS II, data integrity and security.

1a Member States using national copies shall ensure that every access to and all exchanges of SIS II data within these copies are recorded for the purposes specified in paragraph 1.

2. The records shall show, in particular, the history of the alerts, the date and time of the data transmitted, the data used for interrogation, 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.

Article 11 A

Self-auditing

Each authority with a right of access to the SIS II shall have an internal monitoring service responsible for ensuring compliance with this Regulation and reporting directly to its senior management. Each authority shall send a regular report to the national supervisory authority and shall cooperate with them.

Article 11 B

Staff training

Before being authorised to process data stored on 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.

Article 11 C

Communication with the public

Member States shall, in cooperation with their national data protection authority, develop an information policy to inform the general public about the SIS II.

Chapter IIIb

Responsibilities of the Management Authority

Article 12

Operational Management

1. A Management Authority[9] shall be responsible for the operational management of the CS-SIS.
2. The Commission shall be responsible for the operational management of the Communication Infrastructure. It shall settle working arrangements on cooperation procedures with the competent authorities of the Member States and the authority responsible for the operational management of the CS-SIS.
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 CS.SIS. The Commission may[10] entrust the exercise of this management as well as of budget implementing tasks to a national public sector body complying with the following selection criteria:
   (a) it must demonstrate a proven ability to operate a large-scale information system comparable to the second generation Schengen Information System;
   (b) it must possess expertise in the service and security requirements of an information system comparable to the second generation Schengen Information System;
   (c) it must have sufficient staff with the appropriate professional and linguistic skills to work in an international cooperation environment;

---

9 The Justice and Home Affairs Council is to debate and take a view on this question by June 2006 at the latest. Currently four options are taken into consideration (Commission, FRONTEX, EUROPOL, a new European Agency).

10 This provision should be complemented by a Declaration which would make clear that operational management of the CS-SIS is to be delegated. "The Commission has declared that, in order to ensure continuity between the first (SIS 1 +) and second generation (SIS II) of the Schengen Information System, it shall delegate operational management of the CS-SIS during a transitional period before the establishment of the authority responsible for the operational management of the second generation of the Schengen Information System."

(d) it must have an appropriate infrastructure available, in particular with regard to ICT equipment and means of communication; 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 partially or totally to another body 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 CS-SIS shall consist of all the tasks necessary to keep the CS-SIS 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. Operational management of the Communication Infrastructure shall consist of all the tasks necessary to keep the Communication Infrastructure 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.

6. The Management Authority shall ensure that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central SIS II.

Article 13

Security and confidentiality

1. The Management Authority shall, in relation to the Central SIS II and the Communication Infrastructure, adopt the necessary measures in order to:

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment 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 only have access to the data covered by their access authorisation (data access control);

(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, by whom and for what purpose 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 appropriate encryption techniques (transport control).

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

3. 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. This obligation shall also apply after those people leave office or employment or after the termination of their activities.

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 for interrogation, 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 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.

Article 14 AA

Information campaign

The Commission shall 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 individuals. Such campaigns shall be repeated regularly.

Chapter IV

Alerts issued in respect of third country nationals for the purpose of refusing entry

Article 14 A (former Article 16)

Categories of data

1. Without prejudice to Article 8 (1), 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 the 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.[11]
3. (…)[12]

[11] DK and NO underlined they would not accept links between all alerts in the SIS II.
[12] The question of categories of data which may not be processed will be the object of a horizontal provision in the Data protection chapter of this instrument.

Article 14 B

Proportionality clause

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

Article 14 C

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.[13]

(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.

Article 14 D

Minimum data for an alert to be entered

An alert cannot be entered without the data referred to in Article 14 A (2)(k).

Article 15

Conditions for issuing alerts on refusal or entry of 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.

1a Where this decision is taken by an administrative authority, the third country national shall have a right to appeal. Appeals shall be carried out in accordance with national legislation..

[13] The procedure for establishing this data quality standard will be the object of a separate discussion concerning the implementing measures.

2. Decisions may be 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 may 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[14] grounds for believing that he has committed serious criminal offences, including those referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States, or in respect of whom there is clear indication of an intention to commit such offences in the territory of a Member State;

   (c) a third country national who is the object 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.

2a Decisions concerning third country nationals who are beneficiaries of the Community right of free movement within the meaning of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States shall be taken in conformity with legislation adopted in implementing the Directive.

3. Decisions may also be 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 The decisions referred to in paragraph 1 may only be taken on the basis of an individual assessment which shall be documented.

---

[14] A number of delegations entered reserves on the use of the inclusion of the word "serious" and preferred it to be deleted. The Presidency kept this term in regard of the current text of Article 96 SIC.

Article 16

Categories of data

(...)

Article 17

Authorities with right to access the 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;
   (b) other police and customs checks carried out within the country, and the coordination of such checks.
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.
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.

Article 17 A

Limits of access

Users may only search data which they require for the performance of their task.

Article 18

Other authorities with right to access

(...)

Article 18 A

(...)

Article 19

Access to alerts on identity documents

(...)

Article 20

Conservation period of the alerts

1. Personal data 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. The Member State which issued the alert must review the need for continued storage of such data not later than three years after they were entered.
2. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.
3. Alerts shall automatically be erased after three years from the date of the insertion in the CS-SIS.
4. The CS-SIS shall automatically inform the Member States of scheduled deletion of data from the system four months in advance.

4a Alerts issued in respect of a person who has acquired citizenship of any Member State 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.

Article 20 A

Extension of the conservation period of the alerts

The Member State issuing the alert may, within the review period, decide, following an individual assessment, to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the CS-SIS. The provisions of Article 20 shall apply to the extended alert.

CHAPTER V

General data processing rules

Article 21

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 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 Copying for technical purposes as referred to paragraph 2 which leads to off-line databases shall cease one year after the start of operations of the Visa Information System and its communication infrastructure as referred to in Article 38 of Regulation xx/xxxx/EC concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas. Until this date Member States shall keep an up-to-date inventory of these copies, make this available to national data protection supervisory authorities and ensure that all provisions of this Regulation are applied in respect to 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. 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 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.

Article 22

Entering a reference number

(...)

Article 23

SIS II data and national files

1. Article 21 (2) shall not prejudice the right of a Member State to keep in its national files SIS II data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.
2. Article 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.

Article 23 A

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. (…)

Article 24

Quality of the data processed in the SIS II and compatibility between alerts

1. The Member State issuing the alert shall be responsible for ensuring that the data entered into the SIS II is accurate, up-to-date and lawful.
2. Only the Member State issuing the alert shall be authorised to modify, add to, correct 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 advise 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 be obliged to 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 national supervisory authorities involved 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.

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.

Article 24 A

Checking for multiple alerts on an individual

1. Prior to entering an alert the Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics.

2. The following procedure shall be followed:

   (a) if processing a request for entering a new alert reveals that there is already an individual in the SIS II with the same identity description elements a check must be run before the new alert is approved;

   (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.

Article 25

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 originally 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.
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 26

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.

Article 27

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 pursuant to that paragraph, 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.

CHAPTER VI

Data protection

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.

[15]Article 28

Right of information

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.
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 may have factually inaccurate data relating to them corrected or unlawfully stored data relating to them deleted.

Article 29[16]

(...)

---

[15] The application of Directive 95/46/EC as the *lex generalis* on data protection does not prevent the SIS II Regulation from limiting some of the rights contained therein such as the right of information foreseen by Article 11 (1) of the Directive.

[16] DE entered a scrutiny reservation with regard to the deletion of this Article.

Article 30

Remedies

1. Any person may bring before the courts or the authority competent under national law an action 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 32.

Article 31

National supervisory authorities

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 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 1 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 1 have sufficient resources to fulfil the tasks entrusted to them by this Regulation.

2. (…)
3. (…)
4. (…)
5. (…)
6. (…)
7. (…)

Article 31 A

The European Data Protection Supervisor

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 Commission's 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 Commission and the national supervisory authorities referred to in Article 31. The Commission shall be given an opportunity to make comments before the report is adopted.

Article 31 B

Joint responsibilities

1. The national supervisory authorities referred to in Article 31 and the European Data Protection Supervisor shall cooperate actively with each other and bear joint responsibility for the supervision of SIS II.
2. They shall exchange relevant information, conduct joint investigations, including joint 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 European Data Protection Supervisor and the national supervisory authorities shall meet for that purpose at least twice a year. The costs of these meetings shall be borne by 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 and the Commission every two years.

Article 31 C

Data protection during the transitional period

In case the Commission delegates its responsibilities during the transitional period partially or totally to another body 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, to the extent necessary, 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

Article 32

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 requested Member State 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.

Article 33

Sanctions

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

CHAPTER VIII

Final Provisions

[The final provisions are closely connected to the political agreement on the management of SIS II and will therefore be discussed after a final decision.]