►B REGULATION (EC) No 1987/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 December 2006

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

(OJ L 381, 28.12.2006, p. 4)

Amended by:

		Official Journal		
		No	page	date
►M1	Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018	L 295	99	21.11.2018
►M2	Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018	L 312	14	7.12.2018

Corrected by:

►C1	Corrigendum, OJ L 23, 29.1.2015, p. 19 (1987/2006)

▼B

REGULATION (EC) No 1987/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 December 2006

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

CHAPTER I

GENERAL PROVISIONS

Article 1

Establishment and general purpose of SIS II

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

2. The purpose of SIS II shall be, in accordance with this Regulation, to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories, using information communicated via this system.

Article 2

Scope

1. This Regulation establishes the conditions and procedures for the entry and processing in SIS II of alerts in respect of third-country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry into, or a stay in, a Member State.

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

Article 3

Definitions

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

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

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

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

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

  (iii) when the required action cannot be taken;

▼B

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

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

(vi) when dealing with rights of access;

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

(d) ‘third-country national’ means any individual who is neither:

(i) a citizen of the European Union within the meaning of Article 17(1) of the Treaty;

nor

(ii) 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 European Union;

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

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

Article 4

Technical architecture and ways of operating SIS II

1. SIS II shall be composed of:

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

— a technical support function (‘CS-SIS’) containing a database, the ‘SIS II database’;

— a uniform national interface (‘NI-SIS’);

▼B

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

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

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

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

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

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

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

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

Article 5

Costs

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

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

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

▼B

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

▼M2

Article 6

National Systems

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

2. Each Member State shall be responsible for ensuring the uninterrupted availability of SIS II data to end-users.

▼B

Article 7

N.SIS II Office and SIRENE Bureau

1. Each Member State shall designate an authority (the 'N.SIS II Office'), which shall have central responsibility for its N.SIS II. That authority shall be responsible for the smooth operation and security of the N.SIS II, shall ensure the access of the competent authorities to SIS II and shall take the necessary measures to ensure compliance with the provisions of this Regulation. Each Member State shall transmit its alerts via its N.SIS II Office.

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

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

3. The Member States shall inform the management authority of their N.SIS II Office and of their SIRENE Bureau. The management authority shall publish the list of them together with the list referred to in Article 31(8).

Article 8

Exchange of supplementary information

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

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

▼B

3. Requests for supplementary information made by a Member State shall be answered as soon as possible.

4. Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure referred to in Article 51(2) in the form of the SIRENE Manual, without prejudice to the provisions of the instrument setting up the management authority.

Article 9

Technical compliance

1. To ensure the prompt and effective transmission of data, each Member State shall observe, when setting up its N.SIS II, the protocols and technical procedures established to ensure the compatibility of its N.SIS II with CS-SIS. Those protocols and technical procedures shall be established in accordance with the procedure referred to in Article 51(2), without prejudice to the provisions of the instrument setting up the management authority.

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

Article 10

Security – Member States

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

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

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

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

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

▼B

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

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

(g) ensure that all authorities with a right of access to SIS II or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 44(1) without delay upon their request (personnel profiles);

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

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

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

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

▼M2

Article 11

Confidentiality – Member States

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

▼M2

2. Where a Member State cooperates with external contractors in any SIS II-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular on security, confidentiality and data protection.

3. The operational management of N.SIS II or of any technical copies shall not be entrusted to private companies or private organisations.

▼B

Article 12

Keeping of records at national level

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

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

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

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

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

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

▼B

Article 13

Self-monitoring

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

Article 14

Staff training

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

CHAPTER III

RESPONSIBILITIES OF THE MANAGEMENT AUTHORITY

Article 15

Operational management

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

▼M1

2. The Management Authority shall be responsible for all tasks relating to the Communication Infrastructure, in particular:

(a) supervision;

(b) security;

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

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal, and

(f) contractual matters.

▼M2

3a. The Management Authority shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS. It shall provide regular reports to the Member States in this regard.

The Management Authority shall provide a regular report to the Commission covering the issues encountered and the Member States concerned.

The Commission shall provide the European Parliament and the Council with a regular report on data quality issues that are encountered.

▼B

4. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of Central SIS II. The Commission may

▼B

delegate that task and tasks relating to implementation of the budget, in accordance with the Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities [1], to national public-sector bodies, in two different countries.

5. Each national public-sector body referred to in paragraph 4 shall meet the following selection criteria:

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

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

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

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

and

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

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

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

▼M2

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

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

▼M2

running of the system. Those tasks shall also include the coordination, management and support of testing activities for Central SIS II and the N.SIS II that ensure that Central SIS II and the N.SIS II operate in accordance with the requirements for technical compliance set out in Article 9.

▼B

Article 16

Security

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

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

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

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

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

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

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

(g) create profiles describing the functions and responsibilities of persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 45 without delay upon its request (personnel profiles);

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

▼B

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

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

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this 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 17

Confidentiality – Management Authority

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

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

▼M2

3. Where the Management Authority cooperates with external contractors in any SIS II-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular on security, confidentiality and data protection.

4. The operational management of CS-SIS shall not be entrusted to private companies or private organisations.

▼B

Article 18

Keeping of records at central level

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

▼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 searches, the reference to the data transmitted and the name of the competent authority responsible for processing the data.

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

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

5. The competent authorities in charge of checking whether a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to those records for the purpose of fulfilling their tasks.

Article 19

Information campaign

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

CHAPTER IV

ALERTS ISSUED IN RESPECT OF THIRD-COUNTRY NATIONALS FOR THE PURPOSE OF REFUSING ENTRY AND STAY

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS II shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Article 24.

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

▼B

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

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

(c) place and date of birth;

(d) sex;

(e) photographs;

(f) fingerprints;

(g) nationality(ies);

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

(i) reason for the alert;

(j) authority issuing the alert;

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

▼M2

(ka) the type of offence;

▼B

(l) action to be taken;

(m) link(s) to other alerts issued in SIS II in accordance with Article 37.

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 51(2), without prejudice to the provisions of the instrument setting up the Management Authority.

4. The technical rules necessary for searching the data referred to in paragraph 2 shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 31(2).

Article 21

Proportionality

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

▼M2

Where the decision to refuse entry and stay referred to in Article 24(2) is related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant an alert in SIS II. For public

▼M2

or national security reasons, Member States may exceptionally refrain from entering an alert when it is likely to obstruct official or legal inquiries, investigations or procedures.

▼B

Article 22

Specific rules for photographs and fingerprints

The use of photographs and fingerprints as referred to in Article 20(2)(e) and (f) shall be 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 51(2), without prejudice to the provisions of the instrument setting up the Management Authority;

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

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

Article 23

Requirement for an alert to be entered

1. An alert may not be entered without the data referred to in Article 20(2)(a), (d), (k) and (l).

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

Article 24

Conditions for issuing alerts on refusal of entry or stay

1. Data on third-country nationals in respect of 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 taken on the basis of an individual assessment. Appeals against these decisions shall lie in accordance with national legislation.

▼B

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

(a) a third-country national who has been convicted in a Member State of an offence 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 a serious criminal offence or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State.

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

4. This Article shall not apply in respect of the persons referred to in Article 26.

5. The Commission shall review the application of this Article three years after the date referred to in Article 55(2). On the basis of that 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 greater level of harmonisation of the criteria for entering alerts.

Article 25

Conditions for entering alerts on third-country nationals who are beneficiaries of the right of free movement within the Community

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

2. Where there is a hit on an alert pursuant to Article 24 concerning a third-country national who is a beneficiary of the right of free movement within the Community, the Member State executing the alert shall consult immediately the issuing Member State, through 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.

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

▼M2

Article 26

Conditions for entering alerts on third-country nationals subject to restrictive measures

1. Alerts on 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 legal acts adopted by the Council, including measures implementing a travel ban issued by the Security Council of the United Nations, shall, insofar as data-quality requirements are satisfied, be entered into SIS II for the purpose of refusing entry and stay.

2. The alerts shall be entered, kept up-to-date and deleted by the competent authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS II or to alerts entered in accordance with this Regulation, the responsibility shall be taken up by the Member State which holds the subsequent Presidency and which has access to SIS II, including to alerts entered in accordance with this Regulation.

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

▼B

Article 27

Authorities having a right to access alerts

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

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

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

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

3. In addition, the right to access data entered in SIS II and the data concerning documents relating to persons entered in accordance with Article 38(2)(d) and (e) of ►C1 Decision 2007/533/JHA ◄ 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

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

▼B

residence permits and for the administration of legislation relating to 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 law of each Member State.

4. The authorities referred to in this Article shall be included in the list referred to in Article 31(8).

Article 28

Scope of access

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

Article 29

Retention period of alerts

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

2. A Member State issuing an alert shall, within three years of its entry in SIS II, review the need to keep it.

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

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

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

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

▼B

Article 30

Acquisition of citizenship and alerts

Alerts issued in respect of a person who has acquired citizenship of any State whose nationals are beneficiaries of the right of free movement within the Community shall be erased as soon as the Member State which issued the alert becomes aware, or is informed pursuant to Article 34, that the person in question has acquired such citizenship.

CHAPTER V

GENERAL DATA-PROCESSING RULES

Article 31

Processing of SIS II data

1. The Member States may process the data referred to in Article 20 for the purposes of refusing entry into or a 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 27 to carry out a direct search. The provisions of this Regulation shall apply to such copies. Alerts issued by one Member State may not be copied from its N.SIS II into other national data files.

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

Notwithstanding the first subparagraph, technical copies which lead to off-line databases to be used by visa issuing authorities shall no longer be permitted one year after the authority in question has been connected successfully to the Communication Infrastructure for the Visa Information System to be provided for in a future Regulation concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas except for copies made to be used only in an emergency following the unavailability of the network for more than 24 hours.

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

▼B

4. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 27 and to duly authorised staff.

5. Data may not be used for administrative purposes. By way of derogation, data entered in accordance with this Regulation may be used in accordance with the laws of each Member State by the authorities referred to in Article 27(3) in the performance of their duties.

6. Data entered in accordance with Article 24 of this Regulation and data concerning documents relating to persons entered under Article 38(2)(d) and (e) of ►C1 Decision 2007/533/JHA ◄ may be used in accordance with the laws of each Member State for the purposes referred to in Article 27(3) of this Regulation.

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

8. Each Member State shall send to the Management Authority a list of its competent authorities authorised to search directly the data contained in SIS II pursuant to this Regulation as well as any changes to the list. 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*.

9. 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.

Article 32

SIS II data and national files

1. Article 31(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 of national law provide for a longer retention period.

2. Article 31(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS II by that Member State.

Article 33

Information in the event of non-execution of an alert

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

▼B

Article 34

Quality of the data processed in SIS II

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

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

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

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

5. The Member States shall exchange supplementary information if a person complains that he is not the person wanted by an alert. If the outcome of the check is that there are in fact two different persons the complainant shall be informed of the provisions of Article 36.

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

Article 35

Distinguishing between persons with similar characteristics

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

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

▼B

(b) if the cross-check reveals that the subject of the new alert and the person already in SIS II are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 34(6). If the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentification.

Article 36

Additional data for the purpose of dealing with misused identity

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

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

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

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

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

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

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

(c) place and date of birth;

(d) sex;

(e) photographs;

(f) fingerprints;

(g) nationality(ies);

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

▼B

4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established in accordance with the procedure referred to in Article 51(2), without prejudice to the provisions of the instrument setting up the Management Authority.

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

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

Article 37

Links between alerts

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

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

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

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

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

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

7. The technical rules for linking alerts shall be adopted in accordance with the procedure referred to in Article 51(2), without prejudice to the provisions of the instrument setting up the Management Authority.

▼B

Article 38

Purpose and retention period of supplementary information

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

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

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

Article 39

Transfer of personal data to third parties

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

CHAPTER VI

DATA PROTECTION

Article 40

Processing of sensitive categories of data

Processing of the categories of data listed in Article 8(1) of Directive 95/46/EC shall be prohibited.

Article 41

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

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

▼B

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

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

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

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

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

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

Article 42

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 Articles 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 giving rise to the alert, as referred to in Article 24(1).

2. This information shall 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;

▼B

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

Article 43

Remedies

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

2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 48.

3. The rules on remedies provided for in this Article shall be evaluated by the Commission by 17 January 2009.

Article 44

Supervision of N.SIS II

1. The authority or authorities designated in each Member State and endowed with the powers referred to in Article 28 of Directive 95/46/EC (the 'National Supervisory Authority') shall monitor independently the lawfulness of the processing of SIS II personal data on their territory and its transmission from that territory, and the exchange and further processing of supplementary information.

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

3. Member States shall ensure that their National Supervisory Authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

Article 45

Supervision of the Management Authority

1. The European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with this Regulation. The duties and powers

▼B

referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.

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

Article 46

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

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

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

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

Article 47

Data protection during the transitional period

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

▼B

CHAPTER VII

LIABILITY AND PENALTIES

Article 48

Liability

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

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

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

Article 49

Penalties

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

CHAPTER VIII

FINAL PROVISIONS

Article 50

Monitoring and statistics

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

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

3. Each year the Management Authority shall publish statistics showing the number of records per category of alert, the number of

▼B

hits per category of alert and how many times SIS II was accessed, in total and for each Member State.

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

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

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

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

8. 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 3 and 4.

Article 51

Committee

1. The Commission shall be assisted by a Committee.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period provided for in Article 5(6) of Decision 1999/468/EC shall be three months.

3. The Committee shall exercise its function from the date of entry into force of this Regulation.

Article 52

Amendment of the provisions of the Schengen Acquis

1. For the purposes of matters falling within the scope of the Treaty, this Regulation shall replace, on the date referred to in Article 55(2), the provisions of Articles 92 to 119 of the Schengen Convention, with the exception of Article 102 A thereof.

▼B

2. It shall also replace, on the date referred to in Article 55(2), the following provisions of the Schengen acquis implementing those articles ([1]):

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

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

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

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

(e) Decision of the Executive Committee of 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);

(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 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.

Article 53

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 55(2).

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

▼B

Article 54

Transitional period and budget

1. Alerts shall be transferred from SIS 1+ to SIS II. The Member States shall ensure, giving priority to alerts on persons, that the contents of the alerts that are transferred from SIS 1+ to SIS II satisfy the provisions of this Regulation as soon as possible and within three years after the date referred to in Article 55(2) 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 SIS 1+ to SIS II, subject to the following rules:

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

(b) in the event of a hit on an alert transferred from SIS 1+ to SIS II, the Member States shall examine the compatibility of that alert with the provisions of this 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 55(2), which has been approved in accordance with the provisions of Article 119 of the Schengen Convention, shall be paid back to the Member States. The amounts to be repaid shall be calculated on the basis of the contributions from the Member States as laid down in the Decision of the Executive Committee of 14 December 1993 on the financial regulation on the costs of installing and operating the Schengen Information System.

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

Article 55

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*.

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

▼B

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

(a) the necessary implementing measures have been adopted;

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

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

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

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

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

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