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 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.

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 Decision 2006/000/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.

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) 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.

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.

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.