Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 6

National systems

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

Article 7

N.SIS II Office and SIRENE Bureau

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

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

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

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

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

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

Article 8

Exchange of supplementary information

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

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

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

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

Article 9

Technical compliance

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

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

Article 10

Security – Member States

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 11

Confidentiality – Member States

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

Article 12

Keeping of records at national level

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

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

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

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

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

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

Article 13

Self-monitoring

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

Article 14

Staff training

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