COMMISSION DECISION

of 4 May 2010

on the Security Plan for Central SIS II and the Communication Infrastructure

(2010/261/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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) [1] and in particular Article 16 thereof,

Having regard to Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2] and in particular Article 16 thereof,

Whereas:

(1) Article 16 of Regulation (EC) No 1987/2006 and Article 16 of Decision 2007/533/JHA provide that the Management Authority, in relation to Central SIS II, and the Commission, in relation to the Communication Infrastructure, should adopt the necessary measures, including a security plan.

(2) Article 15(4) of Regulation (EC) No 1987/2006 and Article 15(4) of Decision 2007/533/JHA provide that during a transitional period before the Management Authority takes up its responsibilities, the Commission should be responsible for the operational management of Central SIS II.

(3) As the Management Authority has not yet been established, the security plan to be adopted by the Commission should be applicable also to Central SIS II for a transitional period.

(4) Regulation (EC) No 45/2001 of the European Parliament and of the Council [3] applies to the processing of personal data by the Commission when carrying out its responsibilities in the operational management of SIS II.

(5) Article 15(7) of Regulation (EC) No 1987/2006 and Article 15(7) of Decision 2007/533/JHA provide that where the Commission delegates its responsibilities during the transitional period before the Management Authority takes up its responsibilities, it shall ensure that this delegation does not adversely affect any effective control mechanism under Union law, whether of the Court of Justice, the Court of Auditors or the European Data Protection Supervisor.

(6) The Management Authority should adopt its own security plan in relation to Central SIS II once it will have taken up its responsibilities. This security plan should therefore expire, to the extent it relates to the Central SIS II, when the Management Authority takes up its responsibilities.

(7) Article 4(3) of Regulation (EC) No 1987/2006 and Article 4(3) of Decision 2007/533/JHA provide that 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).

(8) The security plan should foresee one System Security Officer performing security-related tasks concerning both Central SIS II and the Communication Infrastructure and two Local Security Officers performing security-related tasks concerning the Central SIS II and the Communication Infrastructure, respectively. The roles of the security officers should be laid down in order to ensure efficient and prompt response to security incidents and reporting thereof.

(9) A Security Policy should be set up describing all technical and organisational details in line with the provisions of this Decision.

(10) Measures should be defined to ensure the appropriate level of security of the operation of Central SIS II and the Communication Infrastructure,

[1] OJ L 381, 28.12.2006, p. 4.
[2] OJ L 205, 7.8.2007, p. 63.
[3] OJ L 8, 12.1.2001, p. 1.

HAS ADOPTED THIS DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Decision establishes the security organisation and measures (security plan) for the protection of the Central SIS II and the data processed therein against threats to their availability, integrity and confidentiality within the meaning of Article 16(1) of Regulation (EC) No 1987/2006 and of Article 16(1) of Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) during a transitional period, until the Management Authority takes up its responsibilities.

2. This Decision establishes the security organisation and measures (security plan) for the protection of the Communication Infrastructure against threats to their availability, integrity and confidentiality within the meaning of Article 16 of Regulation (EC) No 1987/2006 and of Article 16 of Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II).

CHAPTER II

ORGANISATION, RESPONSIBILITIES AND INCIDENT MANAGEMENT

Article 2

Tasks of the Commission

1. The Commission shall implement and monitor the effectiveness of the security measures for Central SIS II referred to in this Decision.

2. The Commission shall implement and monitor the effectiveness of the security measures for the Communication Infrastructure referred to in this Decision.

3. The Commission shall designate a System Security Officer from among its officials. The System Security Officer shall be appointed by the Director General of the Directorate-General for Justice, Freedom and Security of the Commission. The tasks of the System Security Officer shall include in particular:

(a) preparation of the Security Policy as described in Article 7 of this Decision;

(b) monitoring the effectiveness of the implementation of the security procedures of Central SIS II;

(c) monitoring the effectiveness of the implementation of the security procedures of the Communication Infrastructure;

(d) contributing to the preparation of reporting in relation to security as referred to in Article 50 of Regulation (EC) No 1987/2006 and in Article 66 of Decision 2007/533/JHA;

(e) performing coordination and assistance tasks in the checks and audits performed by the European Data Protection Supervisor referred to in Article 45 of Regulation (EC) No 1987/2006 and in Article 61 of Decision 2007/533/JHA, as well as notification of incidents within the meaning of Article 5(2) to the Data Protection Officer of the Commission;

(f) monitoring that this Decision and the Security Policy are applied properly and fully by any contractor including subcontractors being involved in any way in the management of Central SIS II;

(g) monitoring that this Decision and the Security Policy are applied properly and fully by any contractor including subcontractors being involved in any way in the management of the Communication Infrastructure;

(h) maintaining a list of single national contact points for SIS II security and sharing it with the Local Security Officer for the Communication Infrastructure;

(i) sharing the list referred to in (h) with the Local Security Officer for Central SIS II.

Article 3

Local Security Officer for Central SIS II

1. Without prejudice to Article 8, the Commission shall designate a Local Security Officer for Central SIS II from among its officials. Conflicts of interest between the duty of Local Security Officer and any other official duty shall be prevented. The Local Security Officer for Central SIS II shall be appointed by the Director General of the Directorate-General for Justice, Freedom and Security of the Commission.

2. The Local Security Officer for Central SIS II shall ensure that the security measures referred to in this Decision are implemented and the security procedures are followed in the principal CS-SIS. As regards the backup CS-SIS, the Local Security Officer for Central SIS II shall further ensure that security measures referred to in this Decision, except those referred to in Article 9, are implemented and the security procedures relating thereto are followed.

3. The Local Security Officer for Central SIS II may assign any of his or her tasks to subordinate personnel. Conflicts of interest between the duty to execute these tasks and any other official duty shall be prevented. A single contact phone number and address shall allow reaching the Local Security Officer or his or her on-duty subordinate at any time.

4. The Local Security Officer for Central SIS II shall perform the tasks resulting from security measures to be taken at the premises where the principal CS-SIS and the backup CS-SIS are located, within the limits of paragraph 1, including in particular:

(a) local operational security tasks including firewall audit, regular security testing, auditing and reporting;

(b) monitoring the effectiveness of the business continuity plan and ensuring that regular exercises are conducted;

(c) securing evidence on, and reporting to the System Security Officer, any incident in Central SIS II that may have an impact on the security of the Central SIS II or the Communication Infrastructure;

(d) informing the System Security Officer if the Security Policy needs to be amended;

(e) monitoring that this Decision and the Security Policy are applied by any contractor including subcontractors being involved in any way in the operational management of Central SIS II;

(f) ensuring that the staff is made aware of their obligations and monitoring the application of the Security Policy;

(g) monitoring IT security developments and ensuring that staff is trained accordingly;

(h) preparing underlying information and options for the establishment, update and review of the Security Policy in accordance with Article 7.

Article 4

Local Security Officer for the Communication Infrastructure

1. Without prejudice to Article 8, the Commission shall designate a Local Security Officer for the Communication Infrastructure from among its officials. Conflicts of interest between the duty of Local Security Officer and any other official duty shall be prevented. The Local Security Officer for the Communication Infrastructure shall be appointed by the Director General of the Directorate-General for Justice, Freedom and Security of the Commission.

2. The Local Security Officer for the Communication Infrastructure shall monitor the functioning of the Communication Infrastructure and ensure that the security measures are implemented and the security procedures are followed.

3. The Local Security Officer for the Communication Infrastructure may assign any of his or her tasks to subordinate personnel. Conflicts of interest between the duty to execute these tasks and any other official duty shall be prevented. A single contact phone number and address shall allow reaching the Local Security Officer or his or her on-duty subordinate at any time.

4. The Local Security Officer for the Communication Infrastructure shall perform the tasks resulting from security measures to be taken at the Communication Infrastructure, including in particular:

(a) all operational security tasks relating to the Communication Infrastructure, including firewall audit, regular security testing, auditing and reporting;

(b) monitoring the effectiveness of the business continuity plan and ensuring that regular exercises are conducted;

(c) securing evidence on, and reporting to the System Security Officer, any incident occurred in the Communication Infrastructure that may have an impact on the security of the Central SIS II or the Communication Infrastructure;

(d) informing the System Security Officer if the Security Policy needs to be amended;

(e) monitoring that this Decision and the Security Policy is applied by any contractor including subcontractors being involved in any way in the management of the Communication Infrastructure;

(f) ensuring that the staff is made aware of their obligations and monitoring the application the Security Policy;

(g) monitoring IT security developments and ensuring that staff is trained accordingly;

(h) preparing underlying information and options for the establishment, update and review of the Security Policy in accordance with Article 7.

Article 5

Security incidents

1. Any event that has or may have an impact on the security of SIS II and may cause damage or loss to SIS II shall be considered as a security incident, especially where access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed to ensure a quick, effective and proper response in compliance with the Security Policy. Procedures shall be established to recover from an incident.

3. Information regarding a security incident that has or may have an impact on the operation of SIS II in a Member State or on the availability, integrity and confidentiality of the data entered or sent by a Member State, shall be provided to the Member State concerned. Security incidents shall be notified to the Data Protection Officer of the Commission.

Article 6

Incident management

1. All staff and contractors involved in developing, managing or operating SIS II shall be required to note and report any observed or suspected security weaknesses in the Communication Infrastructure to the System Security Officer or the Local Security Officer for the Communication Infrastructure.

2. In case of detection of any incident that has or may have an impact on the security of SIS II, the Local Security Officer for the Communication Infrastructure shall inform as quickly as possible the System Security Officer and, where appropriate, the single national contact point for SIS II security, if such a contact point exists in the Member State in question, in writing or, in case of extreme urgency, via other communication channels. The report shall contain the description of the security incident, the level of risk, the possible consequences and the measures that have been or should be taken to mitigate the risk.

3. Any evidence in relation to the security incident shall be secured immediately by the Local Security Officer for the Communication Infrastructure. To the extent possible under applicable data protection provisions, such evidence shall be made available to the System Security Officer upon request of the latter.

4. Feedback processes shall be defined in the Security Policy to ensure that information about the type, handling and outcome of a security incident is communicated to the System Security Officer and to the Local Security Officer for the Communication Infrastructure, once the incident has been dealt with and is no longer in progress.

5. Paragraphs (1) to (4) shall apply *mutatis mutandis* to incidents in Central SIS II. To that extent, any reference to the Local Security Officer for the Communication Infrastructure in paragraphs (1) to (4) shall be read as a reference to the Local Security Officer for Central SIS II.

CHAPTER III

SECURITY MEASURES

Article 7

Security Policy

1. The Director-General of the Directorate General for Justice, Freedom and Security shall establish, update and regularly review a binding Security Policy in accordance with this Decision. The Security Policy shall provide for the detailed procedures and measures to protect against threats to the availability, integrity and confidentiality of the Communication Infrastructure, including emergency planning, in order to ensure the appropriate level of security as prescribed by this Decision. The Security Policy shall comply with this Decision.

2. The Security Policy shall be based on a risk assessment. The measures described by the Security Policy shall be proportionate to the risks identified.

3. The risk assessment and the Security Policy shall be updated, if technological changes, identification of new threats or any other circumstances make it necessary. The Security Policy shall be reviewed in any event on an annual basis to ensure that it is still appropriately responding to the latest risk assessment or any other newly identified technological change, threat or other relevant circumstance.

4. The Security Policy shall be prepared by the System Security Officer, in coordination with the Local Security Officer for Central SIS II and the Local Security Officer for the Communication Infrastructure.

5. Paragraphs (1) to (4) shall apply *mutatis mutandis* to the Security Policy for Central SIS II. To that extent, any reference to the Local Security Officer for the Communication Infrastructure in paragraphs (1) to (4) shall be read as a reference to the Local Security Officer for Central SIS II.

Article 8

Implementation of the security measures

1. The implementation of tasks and requirements laid down in this Decision and in the Security Policy, including the task of designating a Local Security Officer, may be contracted out or entrusted to private or public bodies.

2. In this case the Commission shall ensure through legally binding agreement that the requirements laid down in this Decision and in the Security Policy, are fully complied with. In case of delegation or contracting out of the task of designating a Local Security Officer, the Commission shall ensure through legally binding agreement that it will be consulted on the person to be designated as Local Security Officer.

Article 9

Facilities access control

1. Security perimeters with appropriate barriers and entry controls shall be used to protect areas that contain data processing facilities.

2. Within the security perimeters, secure areas shall be defined to protect the physical components (assets), including hardware, data media and consoles, plans and other documents on the SIS II as well as offices and other work places of staff involved in operating the SIS II. These secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Work in secure areas shall be subject to the detailed security rules set out in the Security Policy.

3. Physical security for offices, rooms and facilities shall be foreseen and installed. Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled and, if possible, isolated from data processing facilities to avoid unauthorised access.

4. A physical protection of the security perimeters against damage from natural or man-made disaster shall be designed and applied proportionally to the risk.

5. Equipment shall be protected from physical and environmental threats and from opportunities for unauthorised access.

6. If such information is available to the Commission, it shall add to the list referred to in Article 2(3)(h) a single point of contact for monitoring the implementation of the provisions of this Article at the premises where the backup CS-SIS is located.

Article 10

Data media and asset control

1. Removable media containing data shall be protected against unauthorised access, misuse or corruption and its readability shall be ensured during the whole lifetime of the data.

2. Media shall be disposed securely and safely when no longer required, in accordance with the detailed procedures to be set out in the Security Policy.

3. Inventories shall ensure that information on the storage location, the applicable retention period and access authorisations are available.

4. All important assets of the Communication Infrastructure shall be identified, so that they can be protected in accordance with their importance. An up-to-date register of relevant IT equipment shall be kept.

5. An up-to-date documentation of the Communication Infrastructure shall be available. Such documentation must be protected against unauthorised access.

6. Paragraphs (1) to (5) shall apply *mutatis mutandis* to Central SIS II. To that extent, any reference to the Communication Infrastructure shall be read as a reference to Central SIS II.

Article 11

Storage control

1. Appropriate measures shall be taken to ensure proper storage of data and the prevention of unauthorised access thereto.

2. All items of equipment containing storage media shall be checked to ensure that sensitive data have been removed or fully overwritten prior to disposal, or shall be securely destroyed.

Article 12

Password control

1. All passwords shall be kept safely and treated confidentially. In case of suspicion that a password has been disclosed, the password has to be changed immediately or the relevant account has to be disabled. Unique and individual user identities shall be used.

2. Procedures shall be defined in the Security Policy for logging in and out to prevent any unauthorised access.

Article 13

Access control

1. The Security Policy shall establish a formal staff registration and de-registration procedure in place for granting and revoking access to SIS II hardware and software for the purposes of the operational management. The allocation and use of adequate access credentials (passwords or other appropriate means) shall be controlled through a formal management process as laid down in the Security Policy.

2. Access to SIS II hardware and software at the CS-SIS shall:

(i) be restricted to authorised persons;

(ii) be limited to cases where a legitimate purpose in accordance with Article 45 of Regulation (EC) No 1987/2006 and Article 61 of Decision 2007/533/JHA, or with Article 50(2) of Regulation (EC) No 1987/2006 and Article 66(2) of Decision 2007/533/JHA, can be identified;

(iii) not exceed the duration and scope necessary for the purpose of the access; and

(iv) take place only in accordance with an access control policy to be defined in the Security Policy.

3. Only the consoles and software authorised by the Local Security Officer for Central SIS II shall be used at the CS-SIS. The use of system utilities that might be capable of overriding system and application controls shall be restricted and controlled. There shall be procedures in place to control the installation of software.

Article 14

Communication control

The Communication Infrastructure shall be monitored in order to provide availability, integrity and confidentiality for the information exchanges. Cryptographic means shall be used to protect the data transmitted in the communication infrastructure.

Article 15

Input control

Accounts for persons authorised to access SIS II software from CS-SIS shall be monitored by the Local Security Officer for the Central SIS II. Use of those accounts, including time and user identity shall be registered.

Article 16

Transport control

1. Appropriate measures shall be defined in the Security Policy to prevent unauthorised reading, copying, modification or deletion of personal data during the transmission to or from the SIS II or during the transport of data media. Provisions shall be laid down in the Security Policy with regard to the admissible types of dispatch or transport as well as in respect of accountability procedures for the transport of items and their arrival at the place of destination. The data medium shall not contain any data other than the data which is to be sent.

2. Services delivered by third parties involving accessing, processing, communicating or managing data processing facilities or adding products or services to data processing facilities shall have appropriate integrated security controls.

Article 17

Security of the Communication Infrastructure

1. The Communication Infrastructure shall be adequately managed and controlled in order to protect it from threats and to ensure the security of the Communication Infrastructure itself and of Central SIS II, including data exchanged through it.

2. Security features, service levels and management requirements of all network services shall be identified in the network service agreement with the service provider.

3. Besides protecting the SIS II access points, any additional service being used by the Communication Infrastructure shall also be protected. Appropriate measures shall be defined in the Security Policy.

Article 18

Monitoring

1. Logs recording the information referred to in Article 18(1) of Regulation (EC) No 1987/2006 and Article 18(1) of Decision 2007/533/JHA relating to every access to and all exchanges of personal data within the CS-SIS shall be kept securely stored on, and accessible from, the premises where the principal CS-SIS and the backup CS-SIS are located for the maximum period referred to in Article 18(3) of Regulation (EC) No 1987/2006 and Article 18(3) of Decision 2007/533/JHA.

2. Procedures for monitoring use or faults in data processing facilities shall be set out in the Security Policy and the results of the monitoring activities reviewed regularly. If necessary, appropriate action shall be taken.

3. Logging facilities and logs shall be protected against tampering and unauthorised access in order to meet the requirements of collecting and retain evidence for the retention period.

Article 19

Cryptographic measures

Cryptographic measures shall be used where appropriate for the protection of information. Their use, along with the purposes and conditions, must be approved by the System Security Officer in advance.

CHAPTER IV

HUMAN RESOURCES SECURITY

Article 20

Personnel profiles

1. The Security Policy shall define the functions and responsibilities of persons who are authorised to access Central SIS II.

2. The Security Policy shall define the functions and responsibilities of persons who are authorised to access the Communication Infrastructure.

3. The security roles and responsibilities of Commission staff, contractors and staff involved in operational management shall be defined, documented and communicated to the persons concerned. The job description and the objectives shall state these roles and responsibilities for Commission staff; contracts or service level agreements shall state them for contractors.

4. Confidentiality and secrecy agreements shall be concluded with all persons to whom no European Union or Member State public service rules apply. Staff required to work with SIS II data shall have the necessary clearance or certification in accordance with the detailed procedures to be set out in the Security Policy.

Article 21

Information of personnel

1. All staff and contractors shall receive appropriate training in security awareness, legal requirements, policies and procedures, to the extent required by their duties.

2. At the termination of the employment or contract, responsibilities related to job change or employment termination shall be defined for staff and contractors in the Security Policy, and procedures shall be set out in the Security Policy to manage the return of assets and the removal of access rights.

CHAPTER V

FINAL PROVISION

Article 22

Applicability

1. This Decision shall become applicable as of the date fixed by the Council in accordance with Article 55(2) of Regulation (EC) No 1987/2006 and Article 71(2) of Decision 2007/533/JHA.

2. Articles 1(1) and 2(1), Article 2(3)(b), (d), (f) and (i), Article 3, Articles 6(5), 7(5), 9(6), 10(6), 13(2) and (3), Articles 15 and 18 and Article 20(1) shall expire when the Management Authority takes up its responsibilities.

Done at Brussels, 4 May 2010.

For the Commission

The President

José Manuel BARROSO