COMMISSION DECISION

of 4 May 2010

on the Security Plan for the operation of the Visa Information System

(2010/260/EU)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [1], and in particular Article 32 thereof,

Whereas:

(1) Article 32(3) of Regulation (EC) No 767/2008 provides that the Management Authority shall take the necessary measures in order to achieve the objectives in the field of security prescribed in Article 32(2) as regards the operation of the VIS, including the adoption of the security plan.

(2) Article 26(4) of Regulation (EC) No 767/2008 provides that during a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of the VIS.

(3) Regulation (EC) No 45/2001 of the European Parliament and of the Council [2] applies to the processing of personal data by the Commission when carrying out its responsibilities in the operational management of VIS.

(4) Article 26(7) of Regulation (EC) No 767/2008 provides 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.

(5) The Management Authority should set out its own security plan in relation to the VIS once it will have taken up its responsibilities.

(6) Commission Decision 2008/602/EC of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase [3] has described the required security services applicable for the network for VIS.

(7) Article 27 of Regulation (EC) No 767/2008 provides that the principal central VIS, which performs technical supervision and administration functions, shall be located in Strasbourg (France) and a backup central VIS, capable of ensuring all functionalities of the principal central VIS in the event of failure of the system, shall be located in Sankt Johann im Pongau (Austria).

(8) 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 VIS,

HAS ADOPTED THIS DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Decision constitutes the security organisation and measures (security plan) within the meaning of Article 32(3) of Regulation (EC) No 767/2008.

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 VIS and the communication infrastructure referred to in this Decision.

[1] OJ L 218, 13.8.2008, p. 60.
[2] OJ L 8, 12.1.2001, p. 1.
[3] OJ L 194, 23.7.2008, p. 3.

2. 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) the preparation, update and revision of the Security Policy as described in Article 7 of this Decision;

(b) monitoring the effectiveness of the implementation of the security procedures of the central VIS and the communication infrastructure;

(c) contributing to the preparation of reporting in relation to security as referred to in Article 50(3) and 50(4) of Regulation (EC) No 767/2008;

(d) performing coordination and assistance tasks in the checks and audits performed by the European Data Protection Supervisor referred to in Article 42 of Regulation (EC) No 767/2008;

(e) 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 and operation of the VIS;

(f) maintaining a list of single national contact points for VIS security and sharing it with the Local Security Officers for the central VIS and for the communication infrastructure.

Article 3

Local Security Officer for the central VIS

1. Without prejudice to Article 8, the Commission shall designate a Local Security Officer for the central VIS 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 central VIS 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 central VIS shall ensure that the security measures referred to in this Decision are implemented and the security procedures are followed in the principal central VIS. As regards the backup central VIS, the Local Security Officer for the central VIS shall ensure that security measures referred to in this Decision, except those referred to at Article 10, are implemented and the security procedures relating thereto are followed.

3. The Local Security Officer for central VIS 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 central VIS shall perform the tasks resulting from security measures to be taken at the principal and backup central VIS sites, 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 that may have an impact on the security of the central VIS 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 management and operation of the central VIS;

(f) ensuring that the staff are 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 relating to the communication infrastructure, including in particular:

(a) all operational security tasks relating to the communication infrastructure such as, firewall audit, regular security testing, auditing, 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 that may have an impact on the security of the communication infrastructure or the central VIS or on the national systems;

(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 are 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 the operation of VIS and may cause damage or loss to the VIS 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. The Security Policy shall establish procedures to recover from an incident. Security incidents shall be managed to ensure a quick, effective and proper response in compliance with the Security Policy.

3. Information regarding a security incident that has or may have an impact on the operation of VIS in a Member State or on the availability, integrity and confidentiality of the VIS data entered 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 VIS shall be required to note and report any observed or suspected security weaknesses in the operation of VIS to the System Security Officer or the Local Security Officer for the central VIS or the Local Security Officer for the communication infrastructure, as appropriate.

2. In case of detection of any incident that has or may have an impact on the security of the operation of VIS, the Local Security Officer for the central VIS or 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 VIS 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 central VIS or the Local Security Officer for the communication infrastructure, as appropriate. 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 implemented to ensure that information about the results is communicated, once the incident has been dealt with and terminated.

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 VIS, 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 the VIS and the Local Security Officer for the communication infrastructure.

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 VIS as well as offices and other work places of staff involved in operating the VIS. 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(2)(f) a single point of contact for monitoring the implementation of the provisions of this Article at the premises where the backup central VIS 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 central VIS and 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 central VIS and the communication infrastructure shall be available. Such documentation must be protected against unauthorised access.

Article 11

Storage control

1. Appropriate measures shall be taken to ensure proper storage of information 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 user 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 VIS hardware and software at the central VIS 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 VIS hardware and software at the central VIS shall:

(i) be restricted to authorised persons;

(ii) be limited to cases where a legitimate purpose in accordance with Articles 42 and 50(2) of Regulation (EC) No 767/2008 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 VIS shall be used at the central VIS. 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

Control of data recording

Accounts for persons authorised to access VIS software from the central VIS shall be monitored by the Local Security Officer for the central VIS. 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 VIS 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 VIS, 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 VIS 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 34(1) of Regulation (EC) No 767/2008 relating to every access to and all data processing operations within the central VIS shall be kept securely stored on, and accessible from the premises where the principal and backup central VIS sites are located for the period referred to in Article 34(2) of Regulation (EC) No 767/2008.

2. Procedures for monitoring use or faults in information 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 for the evidence 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 the VIS, including the communication infrastructure.

2. 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.

3. 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 VIS 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, where relevant, 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 determined by the Commission in accordance with Article 48(1) of Regulation (EC) No 767/2008.

2. This Decision shall expire when the Management Authority takes up its responsibilities.

Done at Brussels, 4 May 2010.

For the Commission

The President

José Manuel BARROSO