COUNCIL OF
THE EUROPEAN UNION

Brussels, 20 March 2006

7514/06

LIMITE

EURODAC 5

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC

COVER NOTE

from:	European Data Protection Supervisor (EDPS)
Subject:	Inspection report on the first phase of the EURODAC central unit

Delegations will find attached the related report.

Inspection of the EURODAC Central Unit
Report on the first phase

Brussels, 27/02/2006

Postal address: rue Wiertz 60 - B-1047 Brussels, Belgium
Office: rue Montoyer 63, Brussels, Belgium
E-mail: edps@edps.eu.int - Web site: www.edps.eu.int
Tel.:+32-2-283 19 00 - Fax:+32-2-283 19 50

Inspection of the EURODAC Central Unit
Report on the first phase

Introduction

In January 2004, the former Joint Supervisory Body of EURODAC was replaced by the European Data Protection Supervisor ("EDPS"), pursuant to Article 20(11) of Regulation (EC) No. 2725/2000[1], ("the EURODAC Regulation"). As the supervisory authority of the Central Unit, and in compliance with Article 20(2) of the EURODAC regulation the EDPS launched a comprehensive inspection early 2005 consisting of two phases:

1. a first inspection of the Central Unit premises of the overall EURODAC network infrastructure, the results of which are presented in this report;
2. an in-depth security audit of the Central Unit's databases and its premises in order to evaluate whether the security measures implemented still comply with the requirements defined by the EURODAC Regulation (to be realised in the course of 2006).

The EURODAC central system consists of a Central Unit, a Business Continuity System, and three terminal units at two different locations. Network communications between these premises are via the European Commission network (usually named SNET) using VPN boxes to create secure channels. Indeed, the whole EURODAC network infrastructure is hidden from the rest of the Commission. In addition to this, the SNET network has connections with the TESTA II network to allow communications between the EURODAC Central Unit and the Member States local connection points. TESTA II is a private trans-European communication infrastructure managed by Equant and is a component of the IDA program managed by DG ENTR.

This first inspection was conducted in two steps: visits to the EURODAC premises at the two different locations and the submission of a questionnaire to the EURODAC management unit. A meeting was also organised with a representative of the TESTA networks. Based on the facts and elements which have been collected during these two steps and on the related documents which have been analysed, the EDPS inspection team provided an evaluation for each part of the organisation. The description and evaluation parts of the report have been sent for comments to the Commission ; these comments have been analysed. Finally, recommendations have been adopted by the EDPS and included in the final report.

[1] Regulation (EC) 2725/2000 of the Council of 28 February 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

I. Facts and evaluation

The questionnaire submitted to the Commission was built on several sources of information: security standards ISO 17799 and ISO 15408, the EURODAC regulation and especially the Articles 13, 14 and 16, checklists used by the JSA Schengen, as well as Articles 21, 22 and 23 of Regulation (EC) 45/2001[2].

The main objective for the inspection was to gather facts on the implemented security and data protection measures and compare them with the requirements in that field. The efficiency of their implementation will be assessed later by the in-depth security audit foreseen in the second phase of the EDPS inspection.

A. Risks and incidents management

A. 1 Prior to the launch of the system

DELETED

A.2 During the ongoing activities of the system

The EURODAC helpdesk is registering and managing two types of incidents defined according to the EURODAC Regulation:

- Critical incidents which are events that might prevent the Central Unit meeting the operational requirements as defined in the regulation.
- Minor incidents which are of the nature where by the Commission has no control over the resolution.

DELETED

[2] Regulation (EC) No. 45/200 1 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[3] **DELETED**

DELETED

B. Documentation of security

The organisational security policy of EURODAC central unit locations is detailed in a manual.**DELETED**

C. Physical access control

C. 1 EURODA C helpdesk team

DELETED

C.2 Other institutions and on-site contractors

In order to maintain or upgrade the EURODAC systems and premises, access is provided to other institutions or hardware and service providers under specific conditions. **DELETED**

C.3 Visitors

The Policy for visitors is detailed in a dedicated security procedure. This procedure will be assessed during the next phase of the EDPS inspection during the security audit.

D. Logical access control

D. 1 Monitoring access to the system

DELETED

D.2 Monitoring access to the database

DELETED

E. Security of communication

DG JLS maintains an inventory of the equipment under its responsibility as well as a full documentation of the network design which are updated after any configuration and verified once a year. **DELETED**

DELETED

DELETED

F. Information security education and training

DELETED

G. Compliance with the EURODAC regulation

The following part does not specifically concern the level of security of the Central Unit. This part of the questionnaire was aimed at getting a better picture of the activities of the Central Unit, and of the degree to which the EURODAC Regulation is implemented in practice. They contain several elements which the EDPS inspection team considered could be useful for further inspection, either of the Central Unit or of the EURODAC system in Member States.

G. 1 Statistics

The EDPS inspection team asked whether there were statistics available in addition to the mandatory ones provided for in Article 3(3) of the EURODAC Regulation. In particular, statistics on blocking or erasure of data could be of interest. For instance, data must be erased once the Member State of origin becomes aware that the person has acquired citizenship of any Member State; statistics with a breakdown per country could indicate whether this procedure is functioning well.

The EDPS inspection team has been informed that such statistics the publication of which is not provided for by the EURODAC Regulation are collected only for application monitoring / evaluating purposes and are not published.

These statistics were initially not transmitted to the EDPS, for security reasons. However, at a later stage, DG JLS agreed to communicate the statistics the EDPS deems useful either for his supervision of the Central Unit or for the coordinated inspection with national data protection authorities. The EDPS would then be able to communicate these statistics to the national authorities.

Evaluation

The EDPS inspection team is aware of the high level of security required when dealing with sensitive information systems such as EURODAC. The statistical data referred to here is however not considered to be of such a nature that a high level of security is warranted. Refusing communication of such data to the EDPS and national data protection authorities would indeed hamper the effective monitoring and evaluation of the system .

G.2 Implementation of the EURODA C Regulation

The Commission is entrusted with the mission to ensure that the Central Unit is operated in accordance with the provisions of the EURODAC Regulation (Article 13(4), EURODAC Regulation). The EDPS inspection team notes that certain provisions in the EURODAC Regulation, do not seem to have been applied.

a) Direct access to data

Article 4(2) and 15(3) of the Regulation mention different types of access to the data for Member States: direct or via the Central Unit. However, DG JLS has confirmed that there is only one type of access allowed: through the Central Unit. Similarly, Article 4(5) provides for the possibility of direct transmission of the result of a comparison to the Member State of origin (not via the Central Unit). This actually never happens: the result of a request by a Member State is sent to that Member State by the Central Unit.

Evaluation

These two examples tend to demonstrate that the drafters of EURODAC Regulation had envisaged the possibility of direct access and response from the Member States to the database, without using the Central Unit. This possibility is never used, and the text still contains some provisions which are pointless and may create confusion.

b) Destruction of the media used to transferring data

Article 5(2) and 1 1(5.b) provide for destruction of the media used by the Member State of origin for transmitting the data to the Central Unit, once the results of the comparison have been transmitted.

The EDPS inspection team asked how this destruction operation is performed in practice and was informed that this actually never happens, since the only media used for transferring the data is the network. There are no other media such as floppy disks, tapes or paper files.

Evaluation

Here again, it seems that the Regulation provides for a procedure which is not usable in practice. This was important to clarify in the course of the supervision, since the destruction of the media is a responsibility of the Commission.

H. TESTA Network

TESTA provides a secured telecommunication infrastructure that enables the member States as well as the EU institutions bodies to exchange classified information up to the revel of EU RESTRICTED. The network is built on a private dedicated infrastructure on which in an additional IPsec Virtual Private Network is put in place. **DELETED**

DELETED

[4] Council Decision of 19 March 2001 adopting the Council's Security Regulations 2001/264/EC), Official Journal L101, 11 April 2001

[5] Commission Decision of 29 November 2001 amending its Internal Rules of Procedure (notified under document number C(2001) 3031; 2001/844/EC, ECSC, Euratom), "Commission Provision on Security", Official Journal L3 17, 3 December 2001

[6] **DELETED**

DELETED

The s-TESTA network, that will be the successor of TESTA, is currently in the phase of a tendering procedure. It will offer the same level of security, but will also natively provide new security services with proxies and firewalls, higher throughputs, enhanced service level agreements (in particular availability of 99.99%) and a single point of contact for its fully dedicated helpdesk and support services.

DELETED

II Recommendations

The following EDPS recommendations result from the evaluation of the fact-finding step carried out by the EDPS inspection team. They aim at providing guidance and elements for the necessary improvement of the system.

1. **DELETED**

2. **DELETED**

3. **DELETED**

4. **DELETED**

5. **DELETED**

6. A training policy for regular updates in organisational policies and procedures shall be documented and implemented. An awareness training session on data protection requirements shall be added to this newly based regular training policy.

7. The statistics deemed necessary by the EDPS in his supervision task should be transmitted to him upon request. When he deems it useful, the EDPS will communicate these statistics to the competent national data protection authorities, with due respect for appropriate security measures.

8. **DELETED**

9. The EURODAC Regulation contains some provisions which are never applied. Since this may create confusion, e.g. when new users join the system, these provisions should be deleted or redrafted. This recommendation could be part of the results of the general review of the text as undertaken by the Commission in 2006

III Conclusions

The EDPS is generally speaking satisfied with the security level of EURODAC. He welcomes the fact that the Commission is currently revising its procedure and launching various updates which will offer stronger data protection mechanisms. It is of the utmost importance to fully ensure a high level of security of this system, also to maintain its high level of performance.

The EDPS thanks the Commission and especially the responsible officials for their full cooperation during this first inspection of the Central Unit. This inspection also represents an important step in preparing the ground for the coming security audit. The EDPS would like to be informed in due course of any follow-up based on his recommendations the Commission plans to undertake.