EUROPEAN DATA
PROTECTION SUPERVISOR

EDPS Inspection of Eurodac Central Unit

Summary Report

June 2012

1. INTRODUCTION

1.1 Eurodac

EURODAC is a system established under Council Regulation (EC) 2725/2000 (hereinafter "EURODAC regulation") to assist in determining which Member State is to be responsible pursuant to the Dublin Convention[1] for examining an application for asylum lodged in a Member State and otherwise to facilitate the application of the Dublin Convention.

It is used to process data on applicants for asylum, aliens apprehended in connection with the irregular crossing of external borders, as well as aliens found illegally present in a Member State.

The central part of EURODAC consists of a Central Unit (CU) and a backup site (BCU) which includes a test system. Both are located in European Commission buildings in Luxembourg, but they are administered from the main management room in Brussels (DG-Home building). An additional management room and a back-up storage room are located in European Commission buildings in Luxembourg. The central system connects to National Access Points via a secure network.

Under the current management scheme, the European Commission, Directorate General Home Affairs (hereinafter "DG-Home"), is responsible for the operation of the Central Unit of the EURODAC system, whereas the National Access Points are controlled by the relevant Member States' competent authorities.

On 1 December 2012 the management of the EURODAC Central Unit will be transferred to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter "IT Agency"), as provided by Regulation 1077/2011. Until then, the European Commission (DG-Home) remains responsible of the operational management of the EURODAC Central Unit.

1.2 EDPS Supervision of the Eurodac Central Unit

The European Data Protection Supervisor (hereinafter "EDPS"), as established by Regulation 45/2001, monitors the activities of the EU institutions, bodies and agencies in relation to the processing of personal data. To this end, the EDPS is the competent authority for the supervision of the EURODAC Central Unit managed by the European Commission. The duties and powers referred to in Articles 46 and 47 of Regulation 45/2001 apply accordingly.

In addition, Article 20 (11) of the EURODAC Regulation explicitly provides that the EDPS is the supervisory authority for the EURODAC Central Unit and shall exercise all relevant powers as referred to in Article 20 of the Regulation.

1.3 Scope of the inspection

The EDPS performed a first inspection of the EURODAC Central Unit in 2006, followed by a security audit in 2007. This resulted in a list of recommendations with regard to the security of the Central Unit.

[1] Council Decision (EC) 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member states by a third-country national.

The European Commission's DG HOME committed to implement the recommendations in the context of the upgrade to EURODAC plus, which aimed at enhancing performance, quality and security.

The scope of the current (second) inspection was to verify implementation of the EDPS recommendations, and to assess the overall organisational and technical procedures with regard to the protection of personal data and security in EURODAC plus, in accordance with Regulation 45/2001 and the EURODAC Regulation.

The inspection included a security audit and covered the information systems of the operational Central Unit (CU) and the backup site (BCU). The overall data processing operations performed by the EURODAC Central Unit were considered at application, database and server level and relevant organisational, technical and physical security measures were assessed.

The inspection did not involve the network between the Central Unit and the Member States (S-TESTA), nor the underlying network infrastructure of the European Commission (SNET). National interfaces and client facilities used by Members States to gain access to EURODAC were also beyond the scope of this inspection.

1.4 Methodology of the inspection

The inspection plan was based on:

- the EURODAC Regulation, in particular:
    - Article 13 for the responsibility for data use by the Central Unit
    - Article 14 setting out specific requirements for the security of the data processing
    - Article 16 stipulating the keeping of records (EURODAC archiving system)
    - Articles 4-12 for the overall data processing operations performed by the Central Unit (storage of certain categories of data and Member States requests, retention periods for different data categories, etc).
- Regulation 45/2001, in particular the provisions on data quality (Article 4), confidentiality (Article 21) and security of processing (Article 22).
- generally accepted security standards and methodologies (ISO 27000 family).
- the findings of the 2006-2007 EDPS inspection and security audit, as well as the new elements introduced with EURODAC plus.

The inspection was announced in December 2011, and carried out on 27-29 February 2012 in Brussels (2 days) and Luxembourg (1 day), by a team of four representatives from the EDPS and one representative from the Spanish Data Protection Authority.

The EDPS inspectors interviewed key staff members, examined on-the-spot the existing technical, organisational and physical security and data protection controls, and collected electronic evidence. Representatives of the European Commission's DG HOME co-operated and provided assistance.

Comments from DG HOME were taken on board in the inspection minutes, who were then signed both by the EDPS inspectors and DG HOME representatives.

2. SUMMARY AND CONCLUSIONS

The EDPS inspectors found that the overall level of data protection and security of the EURODAC Central Unit is high. The provisions of the EURODAC Regulation with regard to the data processing are being respected (types of data recorded, data retention periods, specific requirements for advance deletion and blocking of data, etc). A specific security policy is being followed, defining clearly the roles and responsibilities of the EURODAC management team and including detailed procedures for several aspects of IT security. A number of technical security measures have been implemented to safeguard personal data at application, database and server levels. Strong physical security measures are in place in all EURODAC locations. Most of the EDPS recommendations made in the 2006-2007 inspection and security audit have been taken into account in EURODAC plus.

This being said, there are some elements which need further improvement in order to assure data protection and security of the overall system.

The EURODAC archiving component was found to be outdated from a technical point of view, and it did not fully take into account specific requirements of the EURODAC Regulation with regard to data retention periods and CAT 3 requests. The archiving component implements the requirement to keep records of all data processing operations within the Central Unit, in order to monitor the admissibility of data processing as well as to ensure data security. As such, it plays an important role and it must be adequately protected against unauthorised access. Furthermore, its records need to be erased after one year, unless they are required for ongoing monitoring procedures.

The business continuity the EURODAC system is based on the failover of the Central Unit to the backup site in case of disaster. This was one one of the main changes introduced with the upgrade to EURODAC plus. Although supported by a Service Level Agreement between DG HOME and DG DIGIT stating that failover from CU to BCU should be tested every year, and by the recommendation of the EDPS (after the security audit performed in 2007) to do this at least every 2 years, no full testing has ever taken place.

Some technical security measures in the area of software patch management, user management, log files, back-ups and system integrity were lacking or found to be inadequate. In particular, the initiative to keep up with operating system level software updates is left to the discretion of the software vendor, who has little incentive to do so. As a result, the system has not been updated yet. Logging in general, both in terms of capturing events and of interpreting the information, was also found to be insufficient.

Some organisational security measures in the area of personal data breach handling, audit, data destruction, change management and maintenance, and policy on removable media were also found to be inadequate. There is for example no specific procedure to handle personal data breaches, including the possible involvement of the DPO, notification of the EDPS (when necessary) and information of Member States' competent authorities where the affected data subjects reside. In violation of the security policy, it was for example also possible to use personal usb storage devices on machines connected to the central system.

Another finding of a broader nature was the fact that the European Commission had not (at the time of the inspection) adopted any specific plans for the transfer of EURODAC to the new IT Agency. Since the transfer itself will have an impact on security, it is extremely important to develop a sound and detailed procedure in order to reduce the risks inherent to the process of taking over as much as possible.

A full report with recommendations was sent to the European Commission, requesting them to provide feedback on measures taken to address the recommendations as soon as possible, and to provide a report on the implementation of those measures should latest by 1 October 2012. The implementation report will therefore be available before the planned transfer to the new IT Agency, which will start operations on 1 December 2012.

Additionally, the EDPS, upon assessment of the implementation report delivered by the Commission, might require that a new security audit be carried out before the handover of EURODAC to the new IT Agency.

Finally, the EDPS announces its intention to make an additional inspection of the EURODAC Central Unit to evaluate data processing activities, in principle, soon after the system is handed over to the IT Agency.