COUNCIL OF
THE EUROPEAN UNION

Brussels, 20 June 2012

11660/12

EURODAC 6

COVER NOTE

<table>
<thead>
<tr>
<th>from:</th>
<th>Ms Giovanni BUTTARELLI, Assistant Supervisor, European Data Protection Supervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>date of receipt:</td>
<td>15 June 2012</td>
</tr>
<tr>
<td>to:</td>
<td>Mr Herman Van Rompuy, President of the Council of the European Union</td>
</tr>
<tr>
<td>Subject:</td>
<td>Eurodac Audit Report - June 2012</td>
</tr>
</tbody>
</table>

Delegations will find attached the Eurodac Audit Report of the European Data Protection Supervisor.
ANNEX

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

President of the Council of the European Union
General Secretariat
Council of the European Union
Rue de la Loi 175
B-1048 Brussels

Brussels, 14 June 2012

Dear Mr President,

As the Supervisory Authority responsible for monitoring that the personal data processing activities of the Eurodac system are carried out in accordance with Regulation (EC) 2725/2000, the European Data Protection Supervisor (EDPS) performed a security audit of Eurodac from 27 to 29 February 2012 at the premises of the EURODAC Central Unit and Business Continuity Unit located in Brussels and Luxembourg.

The aim of the inspection was to verify the implementation of the EDPS recommendations issued in the context of the 2007 EURODAC security audit as well as assess the overall organisational and technical procedures of the European Commission with regard to the protection and security of the EURODAC-related data, in accordance with Regulation (EC) 45/2001 and Council Regulation (EC) 2725/2000.

After having considered the comments received from the European Commission, the EDPS has adopted the final audit report.

Please find attached a copy of the above mentioned report. Our services remain available, should you need any clarification.

Yours sincerely,

Giovanni BUTTARELLI

Cc: Mr Uwe CORSEPIUS, Secretary-General
Annex: Eurodac Audit Report
EURODAC Central Unit

Inspection Report

June 2012

Case file: 2011-1103
INDEX

1. INTRODUCTION
   1.1 The EURODAC system ................................................................. 3
   1.2 EDPS supervision of the EURODAC Central Unit ............................... 3
   1.3 Scope of the inspection ............................................................... 4
   1.4 Methodology of the inspection ...................................................... 4

2. FINDINGS AND RECOMMENDATIONS ....................................................... 6
   2.1 General overview ........................................................................... 6
   2.2 Detailed findings and recommendations ......................................... 6
   2.2.1 Archiving system operation ....................................................... 6
   2.2.2 Business continuity .................................................................... 8
   2.2.3 Technical measures ...................................................................... 8
   2.2.3.1 Software patch management .................................................. 8
   2.2.3.2 User management .................................................................... 9
   2.2.3.3 Log files ................................................................................. 10
   2.2.3.4 Back-ups ............................................................................... 11
   2.2.3.5 System integrity tools ............................................................ 12
   2.2.4 Organisational measures ......................................................... 12
   2.2.4.1 Personal data breach handling ................................................ 12
   2.2.4.2 Security audit ........................................................................ 13
   2.2.4.3 Data destruction ...................................................................... 14
   2.2.4.4 Change management and maintenance .................................... 14
   2.2.4.5 Policy on removable media ................................................... 15
   2.2.5 Transfer to the new IT Agency .................................................... 15

3. IMPLEMENTATION OF THE RECOMMENDATIONS .................................... 17
1. INTRODUCTION

1.1 The EURODAC system

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 Convention¹ for examining an application for asylum lodged in a Member State and otherwise to facilitate the application of the Dublin Convention.

EURODAC consists of a Central Unit, operating the central database of the system, as well as National Access Points for the transmission of data between the Member States and the central database. The data processed through the overall system concern 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 (respectively based on articles 4, 8 and 11 of the EURODAC Regulation).

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.

The EURODAC Central Unit is composed of the operational Central Unit (CU), and the Business Continuity Unit (BCU). A Test system is also available (as part of the BCU infrastructure). Both CU and BCU are located in European Commission buildings in Luxembourg. The EURODAC main management room is located in Brussels (DG-Home building). An additional management room and a back-up storage room are located in European Commission buildings in Luxembourg.

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 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.
1.3 Scope of the inspection

Based on the above-mentioned legal basis, the EDPS performed a first inspection of the EURODAC Central Unit in 2006, followed by a security audit in 2007. As a result of this exercise a list of recommendations were made by the EDPS to the European Commission (DG-Home) with regard to the security of the Central Unit.

The European Commission committed to implement the EDPS recommendations in the context of the upgrade of the EURODAC Central Unit technical architecture (EURODAC plus), which aimed at enhancing the overall system performance, quality and security.

The scope of the current (second) inspection was, therefore, to verify the implementation of the EDPS recommendations issued in the context of the 2006-2007 EURODAC inspection and security audit, as well as assess the overall organisational and technical procedures of the European Commission 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 Business Continuity Unit (BCU) located in Luxembourg and managed in Brussels and Luxembourg by the European Commission (DG-Home). During the inspection the overall data processing operations performed by the EURODAC Central Unit were considered at application, database and server level and the 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) neither the underlying network infrastructure of the European Commission (SNET). National interfaces and client facilities used by Member States to gain access to EURODAC were also beyond the scope of this inspection.

1.4 Methodology of the inspection

The EDPS developed a specific EURODAC inspection plan, including organisational, technical and physical data protection and security controls based on:

1) The existing provisions of the EURODAC Regulation. More specifically, the provisions of the following Articles of the EURODAC Regulation were translated in the inspection plan into specific data protection and security controls:
   - 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).

2) The provisions of Regulation 45/2001 especially on data quality (Article 4), confidentiality (Article 21) and security of processing (Article 22).

3) Generally accepted security standards and methodologies (ISO 27000 family on information security).

4) The findings of the 2006-2007 EDPS inspection and security audit, as well as the new elements introduced with EURODAC plus.

The inspection was officially announced by the EDPS to the European Commission (DG-Home) in
December 2011 together with a request for information on a number of topics identified in the preliminary analysis of the inspection plan. Once this information was received, the EDPS developed the final inspection plan.

The inspection took place on 27-29 February 2012 in Brussels (2 days) and Luxembourg (1 day). The audit team was composed of four representatives from the EDPS and one representative from the Spanish Data Protection Authority.

During the inspection, the EDPS inspectors interviewed key staff members and examined on-the-spot the existing technical, organisational and physical security and data protection controls, following the predefined EUROPAC inspection plan. The representatives of the European Commission (DG-Home) co-operated with the EDPS inspectors and provided the necessary assistance to their tasks.

In the context of the inspection a list of electronic evidence was collected by the EDPS inspectors, after applying hash mechanisms for the integrity of the files.

After the inspection, the EDPS inspectors drafted the Minutes of the inspection, which were sent to the European Commission representatives for comments. Once the comments were received, the final Minutes were produced and signed by both the EDPS inspectors and the European Commission representatives.

The present document is the final report of the inspection.
2. FINDINGS AND RECOMMENDATIONS

2.1 General overview

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 still some elements which need further improvement for the data protection and security of the overall system. More specifically, the EDPS has noted a number of findings regarding:

- The operation of the EURODAC archiving system, which was found outdated from a technical point of view, whereas at the same time specific requirements of the EURODAC Regulation with regard to data retention periods and CAF 3 requests were not fully taken into account.
- The business continuity of the EURODAC system, which has not been fully tested until now (failover between the CU and the BCU).
- The lack or inadequacy of some technical security measures in the areas of software patch management, user management, log files, back-ups and system integrity.
- The lack or inadequacy of some organisation security measures in the areas of personal data breach handling, audit, data destruction, change management and maintenance, and policy on removable media.

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.

The above-mentioned findings are described in more detail in the next Section and specific EDPS recommendations are provided for overcoming the existing problems.

2.2 Detailed findings and recommendations

2.2.1 Archiving system operation

The archiving component plays a central role in the EURODAC system, implementing a specific requirement enshrined in Article 16 of the EURODAC Regulation, i.e. keeping records of all data processing operations within the Central Unit. According to Article 16(2) these records "may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article 14". The records, according to the Regulation, must be protected by appropriate means against unauthorised access and erased after a period of one year, if they are not required for monitoring procedures which have already begun.
**Findings:**

- During the inspection the poor performance of the archiving system was noticed (e.g. long response times to requests), which is due to the ageing of the relevant equipment and software used (in fact this is the only component that has never been updated since the beginning of the EURODAC system).

- The EDPS inspectors verified that the retention period of the archiving system is one year, as stipulated by the EURODAC Regulation. Nevertheless, according to the information provided by the European Commission representatives, this retention policy is not enforced to the back-up tapes of the archiving system, thus allowing the existence of information beyond the legal retention period.

- The EDPS inspectors also noticed that the archiving system stores data records with full fingerprint data (NIST file) for all EURODAC transactions, including CAT 3 requests. However, according to Article 11(5) of the EURODAC Regulation, the NIST file for CAT 3 requests should be deleted immediately after the completion of the search in the central database.

**Possible adverse effects:**

- The ageing of the equipment of the archiving system can potentially lead to breach of the availability and/or integrity of the EURODAC related records.

- The maintenance of back-up files beyond the legal retention period and the recording of CAT 3 NIST files do not fully take into account the requirements of the EURODAC Regulation, as well as the principles of data quality, necessity and minimization under Regulation 45/2001.

**Recommendations:**

- Considering the primary role of the archiving system, the EDPS strongly recommends upgrading it - at both hardware and software level - to put its capacity in line with the rest of the EURODAC system components.

- Considering the requirement of one year retention period of the archiving system under Article 16 of the EURODAC Regulation, the EDPS strongly recommends:
  - a) to delete the information currently stored in the back-up tapes exceeding the legal retention period (i.e. records kept beyond one year);
  - b) to put in place a procedure in order to ensure that the backup policy effectively enforces the requirement of the EURODAC Regulation to the back-up tapes of the archiving system.

In both cases, secure destruction of the data after the end of the processing period should be guaranteed.

- Considering the requirement for immediate deletion of fingerprint data of CAT 3 requests under Article 11(5) of the EURODAC Regulation, the EDPS strongly recommends the European Commission to:
  - a) modify the archiving system in a way that the log files of the CAT 3 transactions are stored without, however, storing the CAT 3 fingerprint data in the overall archiving record;
  - b) delete the NIST files of all CAT 3 requests that are currently present in the archiving system, as well as the back-ups of the archiving system.
2.2.2 Business continuity

Business continuity is concerned with ensuring that critical business functions will remain available during times of emergency. When applied at the level of data centres, it refers to the capability of one data centre taking over from another one. This applies e.g. in the case of a backup data centre configured so as to be able to take over from the primary data centre in case of disaster. This process is known as the failover, and it can be set up to be done either automatically (hot standby), or by intervention from a system administrator (cold standby). It is generally considered to be good practice to actually test failover functionality, preferably in both directions (from primary to backup and vice versa).

EURODAC uses a hot standby business continuity model, which enables CU failover to the BCU in case of disaster. This business continuity model was in fact one of the main components introduced with the upgrade to EURODAC plus, in order to increase the overall availability and integrity of the system and the data therein. In order to guarantee the operation of the business continuity solution, a regular testing of the failover functionality is needed. This is reflected in the SLA between DG HOME and DG DIGIT that states that failover from CU to BCU should be tested every year. The recommendation of the EDPS (after the security audit performed in 2007) has been to do this at least every 2 years.

Finding:

During the inspection it was noticed that no actual live failover has ever taken place between the EURODAC CU and BCU, neither out of necessity nor based on a test. The only case where failover has been tested was during the installation of EURODAC plus. This means that, since the implementation of the new system, no testing of CU failure/BCU recovery has taken place.

Possible adverse effects:

If there is a failure at the CU, failover needs to be initiated without any previous testing. It is then unclear whether the BCU will be able to assume its role, and what practical technical hurdles need to be overcome to do so. In the worst case scenario, attempting to fail over might even worsen the situation at the CU and, thus, greatly affect the availability and integrity of the overall system.

Recommendation:

Taking into account the plans to take EURODAC plus into production and the remaining time between now and the transfer of EURODAC to the new IT Agency, the EDPS strongly recommends the European Commission to seriously consider planning for a failover test during which the EURODAC CU fails over to BCU.

2.2.3 Technical measures

2.2.3.1 Software patch management

Software patch management refers to the practice of updating existing software to fix problems that have been discovered in the course of time, e.g. in the operating system. These problems may include security vulnerabilities and other bugs, and usability enhancements or performance improvements. Software patch management is an essential part of operational security and of the software life cycle in general.

In the case of EURODAC, according to the European Commission representatives, as a matter of policy, only security patches are taken into consideration. The major risk of applying software
patches and/or updates is the possible incompatibility issues that could arise with the Cogent software installed in the EURODAC system (supporting fingerprint analysis). In case a security update would need to be applied, it would be installed on the test system first, and checked by the European Commission running the standard test suite (consisting of 69 checks of system behaviour).

Findings:

- During the inspection it was noticed that no security updates have been applied to date, and software versions have therefore remained the same since 2011.
- It was also stated by the European Commission representatives that should the test suite not complete successfully, it would then be up to the EURODAC contractors (Cogent) to investigate. In general it was confirmed that the overall initiative to monitor and assess security updates, as well as to test and apply them lies thoroughly with the contractors’ consortium (Steria, Bull, Cogent). However, although covered by a maintenance contract, it is unclear where the incentive lies for the contractors to go through the security update process.

Possible adverse effects:

Since the initiative for security upgrades is left thoroughly to the EURODAC contractors' consortium and there is no relevant specific plan or activity from the European Commission's side, there is a real risk that critical operating system patches are not applied and that the operating system will be left vulnerable to known weaknesses. Ultimately this could lead to a situation where operating system level weaknesses are exploited, potentially leading to serious data confidentiality, integrity and/or availability breaches.

Recommendations:

- Operating system level security should receive more attention and better care and should not be considered less important than the Cogent software functionality. To this end, the EDPS strongly recommends that operating system updates are not completely left to the appreciation and initiative of the EURODAC contractors’ consortium and that a clear division of responsibilities between the consortium and the operational system management performed by the European Commission is established.
- In addition, the EDPS strongly recommends that the European Commission develops a software patch management strategy with the aim of keeping a close watch on operating system level security patches by the vendor, taking the initiative to suggest security upgrades, and ultimately forcing those security upgrades that are considered critical in the EURODAC system.

2.2.3.2 User management

User management is crucial in every IT system, as it concerns the creation, modification and deletion of the system’s user accounts and their underlying access rights. This can be considered an explicit requirement for EURODAC under Article 14(1)(e) of the EURODAC Regulation. To this end, the EURODAC system has a detailed user policy in place on how to add, define and authorize a new user, as well as on how to manage and/or delete existing ones, covering both administrative and technical steps.

Finding:

During the inspection the existence in some systems of user accounts corresponding to old users (that are not currently supposed/expected to have access to the system) was noted. According to the information provided by the European Commission representatives, those accounts are maintained
as locked accounts in order to keep a history of the users.

**Possible adverse effects:**
The accidental maintenance of active accounts of non-authorized users (as in the case of old EURODAC users) may endanger the overall operation of the system (e.g. potentially allowing access of unauthorised persons to the system).

**Recommendation:**
Since there is no technical reason for the maintenance of old EURODAC user accounts and considering the possibilities of keeping records of the users by other means (i.e logbook), the EDPS recommends deleting user accounts of users whose presence in the system is no longer justified. As a best practice, the maintenance of a detailed log of the actions related to user accounts plus periodic audits of their validity, access rights and roles is encouraged.

2.2.3.3 **Log files**
Log files are an important security control in every IT system in order to be able to check a posteriori the system/application actions performed by authorised and/or non-authorized users. These files should include all necessary logging information and be appropriately protected from unauthorised access, modification or deletion. The log files should be regularly monitored in order to timely detect any unauthorised system uses.

The activation and use of log files can be considered as an explicit requirement for EURODAC under Article 14(1)(c) of the EURODAC Regulation. In this sense, during the inspection the existence of a specific logging policy covering system and application level events that can be deemed consistent with the requirements of the Regulation was confirmed.

**Findings:**
- Despite the existence of logging policy at system and application level, the EDPS inspectors noticed the absence of logs related to the processing done at database level, including actions performed by administrative users. In the latter case, only references to log-in and log-out events are recorded at application level.
- Regarding security of the logs, with the exception of the intrusion detection feature included in the SMP application, there is no way to ensure that log records cannot be tampered. Even in the case of the intrusion detection system, it was noticed that the system only allows qualifying a log record as not modified, but cannot avoid the deletion of records, whether deliberate or accidental.
- Regarding log analysis and monitoring, it was stated by the European Commission representatives during the inspection that an automated logging monitoring process exists, mainly focused on issues related to the normal operation of the system. In this sense, the process can help notify and escalate events which could impact on the availability of the EURODAC system. Apart from this process, it was confirmed that no other processes to ensure regular monitoring of the logs are in place. This fact should be deemed relevant when considering critical components of the EURODAC system like firewalls.

**Possible adverse effects:**
- The absence of logs at database level, can compromise the overall audit possibility of user activity, taking also into consideration that administrator access at database level qualifies for full access to the data stored in the overall EURODAC system.
• The lack of an integrity mechanism can also compromise the overall use and availability of the logs.
• The lack of log monitoring mechanisms can potentially affect the timely discovery and elimination of security breaches that could affect the overall system functionality, as well as the personal data stored in the system.

Recommendation:
• The EDPS urges the European Commission to enable logging of user actions at database level in the EURODAC system.
• Since log preservation is a capital feature of a sound logging system, the EDPS strongly recommends introducing the changes needed in order to ensure the integrity of the logging system as a whole.
• The EDPS recommends that the European Commission review its logging analysis policy in order to a) identify all systems whose logs should be object of regular examination; b) include as much as possible these logs within the Security Information and Event Management (SIEM) solution in place; and c) develop, when needed, procedures for non-automated review of logs.

2.2.3.4 Back-ups
A backup is a copy of data which may be used to restore the original after a data loss event, e.g. data deletion or corruption. The secondary purpose of back-ups is to restore previous versions of the data as they existed at an earlier time. Therefore back-ups are means to ensure both data availability and overall business continuity of the system. Testing the back-ups (restore) is part of the overall procedure, in order to ensure their usability in case they are needed.

In the case of EURODAC, a detailed back-up policy is in place and back-up tapes are stored in a secure location in Luxembourg. Restore has sometimes taken place for individual files.

Findings:
• During the inspection it was noticed that, although individual files have been restored in the filesystem, no full system restore has ever been tested, nor a restore of databases or of tables in databases. A full system restore poses a different kind of challenge, as it includes information below the filesystem level, and it possibly includes bringing the database(s) into a consistent state.
• A version of the software that was released at the end of 2010 is being used for backup and restore. This means that the upgrade to the most recent release has not taken place, but this should not pose an immediate problem. It may, however, become important at some time in the future.

Possible adverse effects:
It is unclear what the consequences would be in case a full system needs to be restored from the ground up, or in case the database(s) would need to be restored. In an extreme case, the full restore (if performed without prior testing) could potentially threaten the overall system availability and integrity.

Recommendation:
• The EDPS strongly recommends that the European Commission consider testing a full restore of relevant systems, in order to evaluate to which extent they can be brought back into working
order.

- In addition, EDPS recommends that an upgrade of the software used for back-up and restore is performed as soon as possible, in order to avoid performance problems in the future.

2.2.3.5 System integrity tools

The use of system integrity tools enables the detection and reporting of files and changes on servers. Combined with a Security Information and Event Management (SIEM) solution, it becomes possible to correlate and report log and security event data. Therefore, these types of tools support the overall security management and control over the IT system.

Finding:

During the inspection it was noticed that no server integrity tools or equivalent alternative solution are in place in the EURODAC system. In principle it would be up to the European Commission to decide whether such a tool is needed or not, and it would then have to be requested to (and implemented by) the EURODAC contractors' consortium. It should be noted that an older version of the EURODAC Information Security Policy contains a provision on using a tool to check server integrity at regular intervals, and provide reports to the Local IT Security Officer (LISO), but this had been removed from the version that was valid at the time of inspection.

Possible adverse effects:

In case a server's integrity were to be compromised, the absence of the necessary tools could lead to longer time in the detection of the change, possibly worsening the overall consequences to the security of the EURODAC system and the personal data therein.

Recommendation:

EDPS recommends that the European Commission puts server integrity tools in place and integrates them with those tools used in the overall EURODAC security management. This means for example that system alerts need to be generated and sent to identified user roles, and reports need to be evaluated on a regular basis.

2.2.4 Organisational measures

2.2.4.1 Personal data breach handling

Personal data breach handling refers to all the procedures that a data controller has in place in order to detect in a timely manner and resolve a personal data breach, including the notification of all interested parties for possible adverse effects. Following the definition of Directive 136/2009/EC, personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by a data controller.

Finding:

Although the European Commission has an incident handling procedure in place for EURODAC, this does not specifically address personal data breaches. For example, the current procedure does not include steps to assess whether personal data are affected in the course of an incident, involve the DPO, notify the EDPS (if needed) and/or inform the data subjects concerned (through the relevant Member States). Point 8.1 of the Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 provides that "in the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data
processed by Commission information systems, the system owner needs to inform the Data Protection Officer*.

Possible adverse effects:

The lack of a specific data breach handling procedure could result in delays in handling relevant cases, especially with regard to the involvement and information of all the concerned parties (including the affected data subjects).

Recommendations:

- The EDPS recommends that the European Commission establish and document a personal data breach handling procedure (either as part of the incident handling procedure or as a separate procedure), which will describe all the steps to be taken in case that a personal data breach occurs, including the possible involvement of the DPO in accordance with the Implementing Rules for Commission Decision C(2006) 3602, notification of the EDPS (when necessary) and information of competent authorities in Member States where the affected data subjects reside. This procedure should be in line with the European Commission's overall policy on incident and data breach handling.

- In addition, the EDPS recommends that all personal data breaches are adequately documented and maintained in a specific register at the European Commission's premises. The DPO should be able to access the register at any time.

2.2.4.2 Security audit

Auditing (internal and/or external) is a proactive tool for the assessment of an IT system and detection at an early stage of underlying technical or organisational security problems. According to the information provided by the European Commission representatives, the last audit performed in the system was in 2006 by the IAS (with follow-up in 2008) and DG HR-DS. Both of these audits did not include an in-depth security audit of the system.

Finding:

During the inspection it was stated that no recent internal or external security audit of the EURODAC system has been performed and that there were no plans for such an action in the foreseeable future. In addition, it was noticed that in the EURODAC Information Security Policy there is an incorrect reference to the audits carried out by the EDPS. Even though active monitoring and auditing by the EDPS can play a role in order to check and enhance the level of compliance with the EURODAC Regulation, it cannot be seen as a substitute of regular audit practices performed by qualified stakeholders, internal or external.

Possible adverse effects:

The lack of audit mechanisms can compromise the overall security of the EURODAC system, since it is always possible that existing organisational procedures or technical and physical security measures are not operating well and/or an update is needed.

Recommendation:

The EDPS strongly recommends that the European Commission include in its security plan regular audits of the EURODAC system. The EDPS would also welcome any information on the results of such an exercise, including the plans for enforcing recommendations. This will help to reach the goal of proper accountability for the functioning of the EURODAC system.
2.2.4.3 Data destruction

According to Article 4(1)(e) of Regulation 45/2001, personal data should be destroyed after the end of their processing period. The destruction should be performed in a secure way, i.e., in a way that does no longer allows the identification of the data subjects. This can be seen as a measure to ensure primarily the confidentiality of the personal data, in accordance also with Article 14(1)(b) of the EURODAC Regulation. To this end, secure destruction methods should be applied, together with well-defined data destruction procedures once the data have reached the end of their legal retention period.

Findings:

- The European Commission representatives stated during the inspection that electronic data destruction is performed by degaussing and physical destruction of equipment, whereas paper shredders are used for the destruction of physical files. However, it was noticed that no specific procedure is in place in order to describe and detail the steps taken for data destruction (there is only a short reference to data destruction in page 32 of the EURODAC Information Security Policy. For example, there is no detailed procedure on obtaining the formal approval for data destruction, appointing the person responsible for the overall operation, collecting and submitting the media for destruction, signing a data destruction protocol, etc.

- According to the European Commission representatives, no data destruction has ever taken place until now. It was, thus, observed that the hard drives and the back-up tapes of the old EURODAC servers have not been destroyed either, although there is no need to keep the data therein after the transition to EURODAC plus. This material is currently being securely stored in the EURODAC back-up room in Luxembourg.

Possible adverse effects:

- The lack of an established data destruction procedure could put at risk the confidentiality of the personal data to be destroyed (e.g., if the collection and submission of the media for destruction is not monitored by a trusted appointed official).

- In addition, the maintenance of personal data in the old EURODAC servers does not take into account the data necessity and minimization principles under Regulation 45/2001.

Recommendations:

- The EDPS recommends that the European Commission establish and document a specific procedure for the secure destruction of personal data within EURODAC, covering both electronic and paper files.

- Once the data destruction procedure is established, the EDPS recommends the European Commission to apply it for the destruction of the old EURODAC hard disks and back-up tapes that are not currently needed for the operation of the system.

2.2.4.4 Change management and maintenance

Change management and maintenance is important for the management of every IT system, especially when this is distributed and/or many different locations are used. Even small changes should be appropriately recorded, following a specific procedure. EURODAC has a well-established management team that controls changes and takes care of maintenance issues when needed.

Finding:

It was observed during the inspection that all changes (e.g., repair or replacement of equipment)
performed on-the-spot in the CU and BCU sites are registered in specific books and maintained within the sites. It was noted, however, that sometimes these changes may not be communicated to the Brussels management room that is responsible for the overall asset and change management of the sites. This, however, occurs only in cases of minor changes.

Possible adverse effects:
The lack of accurate information could affect the overall asset and change management of the EURODAC sites, potentially resulting in loss of control and/or of data.

Recommendation:
The EDPS recommends that the European Commission develop a procedure for the timely and accurate information of the Brussels management room with regard to any change performed on-the-spot in the EURODAC sites.

2.2.4.5 Policy on removable media
Removable media like USBs provide the possibility of data extraction and, thus, should not be permitted in environments where confidential data are being processed unless this is absolutely necessary for the overall data processing. Moreover, when removable media are activated, appropriate controls should be in place to ensure logging of data recording or data entry performed via these media.

Finding:
During the inspection the European Commission representatives stated that the USB ports in servers and management machines used for EURODAC are generally deactivated and activated only when there is a special need (e.g. transfer of certificates to PostCom). This point is also mentioned in the EURODAC Information Security Policy. However, it was noticed that at the time of the inspection the USB port of one of the EURODAC management machines was activated and, even though Windows audit system was on, it was not possible to find traces of the activation / deactivation process.

Possible adverse effects:
The unnecessary activation of USB ports could potentially lead to extraction of EURODAC information by unauthorised persons, putting at risk the confidentiality of the personal data therein.

Recommendation:
The EDPS advises the European Commission to ensure that the USB ports in EURODAC servers and management machines are activated only when it is absolutely necessary and that the activation/deactivation process is appropriately logged and monitored.

2.2.5 Transfer to the new IT Agency
According to the current planning, the EURODAC system will be transferred at the end of 2012 to the IT Agency. The new locations of the system will, thus, be in Strasbourg (CU) and Sankt Johann in Pongau (BCU).

Finding:
At the time of the inspection there were no concrete developments on the planning for transferring the ownership and management of the EURODAC system to the IT Agency. According to the
information provided by the European Commission representatives, initial contacts were foreseen but concrete plans for the transfer were lacking. Since the transfer process can have an impact on security – depending on the procedures to be adopted, hardware and software components, as well as human resources might be transferred to the IT Agency – 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.

Possible adverse effects:
The lack of an accurate planning for the timely transfer of EURODAC to the IT Agency might endanger the availability, as well as the overall security of the system.

Recommendation:
The EDPS encourages the European Commission to start the planning of the EURODAC transfer as soon as possible having in mind the need to ensure proper transfer of the assets, business continuity and the highest level of availability. In this respect, the EDPS would welcome further information with regard to the development and implementation of the transfer.
3. IMPLEMENTATION OF THE RECOMMENDATIONS

Following the recommendations mentioned in Chapter 2 of this document, the EDPS expects the European Commission to implement as soon as possible the following measures:

- Archiving system operation:
  - Introduce a specific plan for the upgrade – at both hardware and software level - of the archiving component of the EURODAC system.
  - Delete the information currently stored in the back-up tapes of the archiving system which exceeds the retention period of one year.
  - Put in place a procedure in order to ensure that the retention period of the archiving system records stored in back-ups does not exceed one year.
  - Introduce a plan for the modification of the archiving system with regard to CAT 3 requests, in a way that the log files of the transactions are stored but without storing the CAT 3 fingerprint data (NIST file) in the overall record.
  - Delete the NIST files of all CAT 3 requests that are currently present in the archiving system, as well as the back-ups of the archiving system.

- Business continuity:
  - Introduce a specific plan for the performance of a failover test from EURODAC CU to BCU before the transfer of the overall system to the IT Agency.

- Software patch management:
  - Develop a software patch management strategy with the aim of keeping a close watch on operating system level security patches by the vendor, taking the initiative to suggest security upgrades, and ultimately forcing those security upgrades that are considered critical in the EURODAC system.
  - Clarify the responsibilities on software patch management between the European Commission EURODAC management team and the EURODAC contractors' consortium.

- User management:
  - Delete user accounts whose presence in the system is no longer justified. As a best practice, the maintenance of a detailed log of the actions related to user accounts plus periodic audits of their validity, access rights and roles is encouraged.

- Log files:
  - Enable logging of user actions at database level in the EURODAC system.
  - Introduce the changes needed in order to ensure the integrity of the logging system as a whole.
  - Review the existing logging analysis policy in order to a) identify all systems whose logs should be object of regular examination; b) include as much as possible these logs within the SIEM solution in place; and c) develop, when needed, procedures for non-automated review of logs.

- Back-ups:
  - Introduce a specific plan for testing a full back-up restore in EURODAC before the overall system's transfer to the IT Agency.
- Introduce a specific plan for the upgrade of the software used for back-up and restore.

- System integrity tools:
  - Consider the possibility of putting server integrity tools in place and integrating them with those tools used in the overall EURODAC security management.

- Personal data breach handling:
  - Establish and document a personal data breach handling procedure (either as part of the incident handling procedure or as a separate procedure), which will describe all the steps to be taken in case that a personal data breach occurs, 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.
  - Ensure that all personal data breaches are adequately documented and maintained in a specific register at the European Commission's premises. The DPO should be able to access the register at any time.

- Security audit
  - Introduce a specific plan for regular audits of the EURODAC system as a measure of accountability.

- Data destruction:
  - Establish and document a specific procedure for the secure destruction of personal data within EURODAC, covering both electronic and paper files.
  - Introduce a specific plan for the destruction of the old EURODAC hard disks and back-up tapes (that are not currently needed for the operation of the system) before the transfer to the IT Agency.

- Change management and maintenance
  - Develop a procedure for the timely and accurate information of the Brussels management room with regard to any change performed on-the-spot in the EURODAC sites.

- Policy on removable media:
  - Ensure that the USB ports in EURODAC servers and management machines are activated only when it is absolutely necessary and that the activation/deactivation process is appropriately logged and monitored.

The European Commission should report to the EDPS on the implementation of the above-mentioned measures latest by 1 October 2012.

In addition to the above measures, the EDPS encourages the European Commission to start the planning of the EURODAC transfer to the IT Agency as soon as possible having in mind the need to ensure proper transfer of the assets, business continuity and the highest level of availability. In this respect, the EDPS would welcome further information as soon as this is available with regard to the development and implementation of the transfer.

Moreover, considering that this report will be issued while developing the taking over process, the EDPS recommends the European Commission to include in the documentation of the transfer both a copy of this report and a progress report on the adoption of the EDPS recommendations, so as to
enable the IT Agency to continue with the follow up.

The EDPS will review the proper implementation of the recommendations of the inspection report and will closely monitor the transfer of the EURODAC system from the European Commission to the IT Agency.

The EDPS will also assess in due course the need for the performance of a new inspection after the transfer of the system to the IT Agency.