**Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on Access Control System at JRC Ispra Site.**

Brussels, 15 July 2011 (Case 2010-0902)

## 1. Proceedings

On 15 November 2010, the European Data Protection Supervisor ("*EDPS*") received from the Data Protection Officer ("*DPO*") of the European Commission a notification for prior checking ("*the Notification*") regarding the data processing operations relating to the Access Control System at JRC Ispra Site.

The following documents were attached to the notification:
- Legislative Decree of the Government 17 March 1995 n° 230 (in IT);
- Law n. 906 of 1st August 1960 establishing formal agreement between EC and Italy (in IT);
- Ministry of Industry Decree of 21.07.87 with technical specifications (confidential n. 42) (in IT);
- Mission Statement of the Security Service JRC Ispra, 23 February 2007;
- Diagram describing the interaction between existing Security Service Information Systems with details regarding each system's main functional or data modules;
- Privacy Statement on the Access Control System at JRC Ispra.

On 30 November, the EDPS made a request for further information. The EDPS sent reminders of this request on 7 February and 7 March 2011. The suspension of the procedure was eventually lifted on 10 March 2011, when additional information was provided to the EDPS regarding the legal basis. An additional request for further information was made on 16 March and replied on 18 March 2011. On 20 April 2011, due to the complexity of the matter, the EDPS decided that the deadline to provide his Opinion would be extended by one month.

On 18 May 2011, the EDPS sent the draft Opinion to the DPO of the European Commission for comments. The comments were only received on 8 July 2011.

## 2. Examination of the matter

### 2.1. The facts

2.1.1 Description of the processing

According to the notification, the **purpose** of the Access Control System at JRC Ispra, one element of the Physical Protection Systems installed on site, is to protect the European

Commission premises in Ispra against unauthorised access and against external as well as internal threats. It is essentially composed of end point technical components (card readers connected to the badges used by staff members and alarm points) installed throughout the campus, the sites entrances as well as its perimeter fence. Such installations use databases as information sources and repositories in order to implement and enforce access controls.

The Access Control System covers not only the entrances to the site, but also access to other more restricted areas like Nuclear Areas or certain Research Laboratories.

To the EDPS, another important element of the notification is that access to some protected areas (Security office and local control room) of the JRC premises will be covered by biometric readers (4 in total) and only some staff members will be using biometric readers (staff members of the Security Office and guards at the entrance).

In entrances to the site where it is possible to enter with vehicles, the JRC plans to implement a vehicle licence plate recognition system to verify that vehicles entering the site are effectively registered in the Vehicle Registration module of SECPAC (Case 2007-0381) and are thus authorised to enter the site.

According to the data controller, independently of the technology used, no other information apart from the physical badge number is read from or stored on the badge.

The access control system aims at providing:

- Security measures to protect the persons and premises of the site.
- Authorisation of access to site (registration of staff, visitors and vehicles),
- Physical protection of the site (guards, alarms, video surveillance, etc.)
- Protection of Commission assets, information and monitoring of information system security.

As to the access control based on biometric, the biometric system fulfils the following purposes:

- As to the Security Office, it protects the Security Service 'Data Centre' rooms, hosting servers in well protected highly secure Access Controlled Areas where there is a presence of a limited number of vetted *Security Staff* or *Guards* that have instructions to accompany at all times and monitor activities of anyone temporarily allowed to enter such areas.

- As to the local control room, the JRC informed the EDPS that due to the location (publicly accessible at main entrance next to the Reception area) and sensitivity of the area (several important Physical Protection Systems are accessible form within that room), it is imposed that the door of the Security local room is kept closed at all times, and that everyone is correctly and clearly identified.

**Legal basis**: According to the notification, the processing is necessary in order to comply with Italian Law concerning Nuclear Sites and both Commission and JRC internal regulations concerning On-Site Presences.

JRC submitted the following elements forming the legal basis of the processing:

International Legislation

- IAEA INFCIRC/255 Prescription (http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html)
- EURATOM Regulation n. 3 (O.J. 406/58 of 06.10.58)
- Law n. 906 of 1st August 1960 establishing formal agreement between EC and Italy
- Ministry of Industry Decree of 21.07.87 with technical specifications (confidential n. 42)

Internal Rules and Regulations
- 72 month On-site Presence rule (C(2004) 1597) along with JRC specific rules.
- Security Provisions C(2001) 3031 of 29.11.2001
- Industrial Security C(2006) 548 of 02.08.2006
- IT Security C(2006) 3602 0f 16.08.2006
- Mission Statement of Security Service

**Automated/manual processing:** The programming of all existing card readers is usually performed automatically on a daily basis but may be performed manually in case of need if urgent updates are needed[1].

Similarly for what concerns automated vehicle access control, dedicated cameras read the licence plate -by taking several image snapshots using OCR technology to interpret it- and confront the result with the records regarding registered and thus authorised vehicles. Furthermore a wider image of the entrance or entrance lane is visible and captured in order to verify the number of occupants of a vehicle corresponds to the number of badges identified and also present an overview of what is happening. According to the notification, such a system does not have as an aim the identification of people transiting.

Transactions from the readers i.e. date and time, eventual direction (entry or exit) and badge number are automatically registered within the ARDOS database. All anomalies i.e. unauthorised access attempts, expired card usage, technical malfunctioning, etc. are also registered within the same database.

A limited number of real-time transactions are visible to the guards in key points of entry to the site. Guards don't have access and are thus not allowed to modify or search within such data but can visualise the list of people present and print in case of need an Emergency Evacuation List.

[...]

The definition of Card Readers and their relationship in micro or macro 'Virtual Areas' is also performed manually following 'in the field' logic.

As regards the **data subjects** concerned, the processing covers anyone needing to access, enter or visit the Joint Research Centre-Ispra Site.

Only Security Service staff members and guards at the entrance are concerned with processing operations using biometric readers. This includes 12 members of Core Security Service staff currently enrolled in the group of 3 readers used in the main Security Building Areas and 40 Guards at the main entrance using one reader. This reader provides quick access to the Local Control Room. Comments on the draft opinion made on behalf of the data

[1] Such a processing involves the reading of all active 'staff pass' and 'special authorisation' request data from SECPAC and transformation of such data to a binary format understood by the card readers.

controller stressed that the biometric readers system amounts for less than 1% of the components of the JRC Access Control System. To the EDPS, the size of the system or the number of people concerned by a system processing biometric data shall not prevent the full compliance of the system with the Regulation.

Data fields to consider are mainly related to transactions and anomalies associated with a physical badge number that is then associated with a staff member or visitor. The **data** which are processed are the following:

- Staff Pass or Special Authorisation Data Fields are covered by SECPAC (Case 2007-0381) and ARDOS (Case 2007-0380).

- Physical Badge: Badge Num, PIN Code, Version (augmented when badge lost or stolen), Validity Dates

- Card Reader: Reader ID, Description, Physical Location, Location Co-ordinates, Parent Reader or Area

- Special Authorisation: Badge Num, Validity Dates (Max. 14 months), Time Range Validity (Working hours up to 24h/24h and Working Days up to 365 days/year), Accessible Areas (Buildings, Offices, Specific Reader IDs).

Furthermore data from card readers and licence plate recognition system (when implemented), related to Transactions and Anomalies are collected:

- Badge Transaction: Badge Num., Reader ID, Date, Time, Direction (Entry/Exit)

- Badge Anomalies: Badge Num., Reader ID, Date, Time, Error Code and Error Message

- Vehicle Transaction (automated recognition): Plate Number, Data Reliability, Plate Nationality (indicative), Time, Direction (Entry/Exit), Anomaly Flag with eventual corrected Plate Number.

The Access Control System is the end point system receiving data from SECPAC and ARDOS. The data of the Access Control System that ends up in the ARDOS database for what concerns card reader transactions is by definition not used for presence control or flexitime accounting.

According to the notification, **a privacy statement** about the general access control system is available to the data subjects in a clear visible way on the JRC intranet.

According to the data controller, the following **recipients** may process the data:

- Only selected staff of Security Service may have access to all the personal data used in this system as well as all information in the SECPAC information system. Information based on Access Control Data can be handed over to national law enforcement agencies upon written request and duly authorized by the controller in case of crime prevention or investigations regarding threats to Security, the JRC sites or the European Commission.

- The Security Service, responsible for managing access to the Ispra site, may also transfer data for security reasons to the Security Directorate (DG HR/DS) of the Commission.

- For contractual invoicing reasons, the data on real presence (in connection with SECPAC) on site of staff working for external contractors could be transferred to all Management Support Units (MSU) on the Ispra site.

According to the notification, information is provided always with a very good justification on the basis of the 'need to know' principle. Data are provided mainly for internal use of Security Service.

Regarding **storage**, data is currently kept on direct access storage of Security Service servers connected to the Security Service internal network, physically disconnected and not accessible from the outside world, as well as on removable media used for backup purposes.

Regarding the biometric data, fingerprint templates are stored exclusively on the biometric readers dedicated memory. The actual biometric reader included in the 4 mentioned Access Control Readers is connected locally to the Access Control Reader main board.

Regarding **retention** of the data, access Control System transaction and anomaly data has only been kept since 2002 in its present format. Being complimentary to daily permit, staff pass and special authorisation related information, the data controller considers that these data should be kept for at least 12 years[2].

After the standard retention period of 12 years, data related to general access control transactions will be anonymised in order to be able to produce statistics.

Regarding the registration of controlled zones or nuclear areas entry/exit, the duration of the retention period is 30 years due to legal requirements e.g. to store Dosimeter assignments for health reasons.

The **rights of the data subjects** are implemented as follows: upon justified request from the data subject data will be modified, frozen or eventually erased in a maximum period of one month.

This processing of personnel data is under the responsibility of the Head of Unit for Safety and Security. This HoU reports directly to the Ispra Site Director.

**Technological system:**
[...]

## 2.2. Legal aspects

### 2.2.1. Prior checking

This prior check Opinion relates to processing of personal information carried out by JRC, in particular the Security Services, to ensure that only authorised persons have access to JRC

[2] This covers the access logs, which are kept for what concerns accesses to the Access Control System application.

perimeter. It covers card readers systems, biometric identification and CCTV footages performed during vehicle registration.

***Applicability of the Regulation.*** The notification concerns the processing of personal data, within the meaning of Regulation (EC) No 45/2001.

It involves the collection, recording, organisation, storage, retrieval, consultation, etc. of personal data (Article 2(b)) within the context of the management of access control at JRC premises. These activities constitute partially automated and partially manual processing operations by a body of the EU (former "community body") insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of former "Community law" (Article 3 of the Regulation, in the light of the Lisbon Treaty). The processing therefore falls within the scope of Regulation (EC) No 45/2001.

***Grounds for prior checking***. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*.

The EDPS wishes to stress that in most of the cases, he would not prior-check access control processing operations as they would normally not fall under Article 27[3].

However, the EDPS also considers that the presence of some biometric data other than photographs alone, such as the case in point where biometric fingerprints are collected, presents specific risks to the rights and freedoms of data subjects[4]. This position is mainly based on the nature of biometric data which is highly delicate, due to some inherent characteristics of this type of data. Biometric data changes irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. In addition to that, the EDPS also notes that possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for data subjects. These risks justify the need for the data processing to be prior checked by the EDPS in order to verify that stringent safeguards have been implemented.

Regarding the use of vehicle licence plate recognition system at the entrance of the JRC area, the aim is to verify that vehicles entering the site are effectively registered in the Vehicle Registration module of SECPAC and are thus authorised to enter the site.

The JRC underlined that "*a wider image of the entrance or entrance lane is visible and captured in order to verify the number of occupants of a vehicle corresponds to the number of badges identified and also present an overview of what is happening. It should be noted that such a system does not have as an aim the identification of people transiting.*"

To the EDPS, such processing is a processing of personal data which could also be a monitoring system and should be considered in the framework of the Videosurveillance Guidelines. Therefore, given the purpose of the processing operation of this system and the process taking place, the EDPS wants to remind the JRC that it needs to comply with the EDPS Videosurveillance Guidelines, which were adopted on 17 March 2010 and for which impact assessments were supposed to be sent to the EDPS by 1 January 2011. The EDPS invites the JRC to comply with this requirement as soon as possible regarding the planned

[3] See for instance case 2009-0382 on the Security access system of the Fundamental Rights Agency and case 2009-0639 on the Identity & Access Management of the Court of Auditors, to be found on the EDPS website.
[4] See also case 2007-0501 Iris scan system at the European Central Bank and case 2007-0635 Access control at OLAF

used of CCTV at the JRC sites. This part of the access control system will not be dealt with here.

***Ex-post Prior Checking.***

Since prior checking is designed to address situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. In this case however the processing operation has already been established.

By consequence, the EDPS considers that the JRC **is in breach of the Regulation** since it installed and ran a biometric access control system without notifying the planned processing operation to the EDPS. Therefore, the EDPS urges the JRC to implement the conclusions of this Opinion as soon as possible to be in conformity with the Regulation

The notification was received on 15 November 2011. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 102 days + one month extension to obtain additional information plus 51 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later than 18 July 2011 (17 July being a Sunday).

### 2.2.2. Lawfulness of the processing

Personal data may only be processed if grounds can be found in Article 5 of Regulation (EC) No 45/2001.

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed".*

Moreover, the JRC states that Article 5 b) also applies in this situation as the "*processing is necessary for compliance with a legal obligation to which the controller is subject*".

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001, three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out; second, whether the processing operations are performed in the public interests; and, third, whether the processing operations are indeed necessary for the performance of that task (necessity test). Obviously, the three requirements are closely related. As to the compliance with Article 5 b), an analysis of the legal obligation to which the controller is subject should be conducted.

* The **legal basis** mentioned by the JRC (see the facts above) combines international and national legislations as well as EU internal rules and regulations. The EDPS requested the JRC to provide a justification as to the relevance of the said legal instruments for the processing. JRC provided it for each legal instrument stated in the notification. Here, the EDPS makes a difference between the general access control system and the biometric access control.

As analysed by the EDPS, the various legal acts describe general measures to implement an access control system and can be considered as a sufficient legal basis covering such processing operations.

However, the EDPS considers that the different legal acts presented remain very general as regards the processing operations using a fingerprint technology for access control. The setting up of an access control system is a measure that relates to the organization of the JRC, which in its view is necessary in order to optimize the security and overall functioning of the JRC. However, because the setting up of an access control system based on fingerprint technology is particularly intrusive to the privacy of individuals, the EDPS considers that the JRC should adopt another more specific legal basis foreseeing the specific processing operations at stake, using biometric data. This should be carried out pursuant to a specific administrative act of the institution, which would set the conditions of use of such system.

Similarly, the legal obligation to which the data controller is subject following Article 5 b) is imposed by national legislation, which is also very general and does not, for instance, foresee specifically the use of biometric systems/technology for access control. For this reason as well, the specific legal basis that the JRC has to adopt should also take the national obligations as references.

* As to the necessity of the processing **(necessity test),** according to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. In this respect, recital 27 of Regulation (EC) No 45/2001 states that: "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*".

From the explanations and clarifications provided by the JRC, the EDPS concludes that JRC is entitled to implement:

- physical protection measures that are applicable to sensitive installations and laboratories;
- obligatory registration of who is present on-site;
- a physical protection plan when extra security measures would be deemed necessary to mitigate specific threats or risks;
- measures to protect information processing facilities.

Taking into account the relevance of these interests and in order to prevent the unauthorized access, the JRC could indeed find it necessary to adopt special security measures, including the setting up of stringent access control systems for specific areas of the JRC.

However, taking into account the described nature of the biometric data processed (as outlined above in section 2.2.1), to properly assess the adequacy of the use of such data for access control purposes it is necessary to carry out a ***targeted impact assessment,*** evaluating the reasons that justify the use of such technique and whether other, less privacy intrusive alternatives, were envisaged. When analysing the need for the current biometric system, the main argument presented by the JRC relates to the fact that the system shall facilitate a quick access to specific dedicated rooms for which such access has to be done in a swift, quick, reactive way. The JRC justifies that with the high flux of transits in and out of the room the use of a badge coupled with the need to type a 4 digit PIN code (not considering also eventual risks like shoulder surfing, etc.) would have taken more time for opening the door than the use of a fingerprint reader that immediately verifies authorisation and identifies the person wanting to access that area.

Therefore, the justification for the processing relates more to a question of quick accessibility than security. Vis-à-vis the future and particularly concerning possible updates of the system (see below under "Accuracy"), the EDPS considers that the JRC should conduct a targeted impact assessment where privacy/data protection considerations should be more prominently taken into account.

### 2.2.3. Processing of special categories of data

The notified data processing does not relate to data falling under the categories of data referred to in Article 10.1 of Regulation (EC) No 45/2001. The EDPS wants to underline that in the case of impossibility to enrol in the biometric reader system for health reasons (for instance because a health treatment would not allow the possibility to use fingerprints that would be damaged), Article 10 of the Regulation should be applied.

### 2.2.4. Data quality

***Adequacy, relevance and proportionality.*** Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed. This is referred to as the data quality principle. In analyzing whether the processing at point, which also involves, for some dedicated areas of the premises, the processing of biometric data, is in line with this principle, the EDPS notes the following.

The type of data collected, mainly the fingerprints and related identification information, corresponds to the data required to operate an access control system based on processing of biometric data. From this point of view, the data collected are adequate and relevant for the purposes of the processing.

Moreover, the EDPS acknowledges that JRC observed the Need-To-Know principle by enrolling only the people who need special access to ensure that only authorised persons have access to certain sensitive areas of the JRC.

***Fairness and lawfulness.*** Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analyzed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects who is further addressed in Section 2.2.8.

***Accuracy.*** According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date"*, and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified"*.

In this case, the personal data at stake include mainly identification data, used for access control purposes.

As already explained above, for some staff members (those who need to access the Security office and the local control room), it includes biometric data. Some key features of biometric systems have a direct impact on the level of accuracy of the data generated either in the enrolment or identification phases inherent to this type of system. Depending on whether biometric system is set up in a way that integrates these key elements, the accuracy of the data

will be (or not) at stake. Next we describe these key elements and analyze the extent to which they have been taken into account in the biometric system concerned.

Firstly, the enrolment phase must foresee alternative ways to identify individuals who are not eligible for enrolment, for example because of damaged fingerprints. This is usually referred to as ***"fall back procedures"***[5]. Similar types of measures must be foreseen for those individuals who are properly enrolled but who are wrongly identified (usually referred to as "***false rejection***").

The EDPS notes that an alternative card reader, either based on magnetic band or Mifare, is used in parallel to the fingerprint reader in 3 of the 4 locations. For such an alternative reader it is necessary to always use the associated staff pass PIN. In case of an emergency a backup key that is kept in a sealed envelope within a safe, gives also access to this zone. The safe is accessible only to 2 members of Security Service.

From the JRC experience the False Rejection Rate (FRR) is extremely low. When the system rejects an entrance it is because the person is not authorised, not correctly placing their finger on the fingerprint reader or is using the wrong finger. Such issues are usually followed-up straight away by Security Staff that have never actually seen FFR problems 'in the field'.

Regarding the accuracy of the data, the JRC has not conducted a depth study on the false acceptance and rejection rates for the whole system it has implemented. Therefore, the JRC should provide the EDPS with the FRR established by the Security Service Contractor as well as the operational FRR, which is effectively used.

The EDPS notes that the use of biometrics for identification and access control purposes using the "comparison one to many" search mode does not always lead to correct results. In other words, it may misidentify individuals and thus create inaccurate records. An alternative search mode such as the "one to one" does not present the same problem because the biometric data are only compared to one template rather than being compared to a larger number of templates. The "one to one" search mode usually involves the storage of the template in a chip. However, the template can also be stored in a central database but in this case it must be accompanied by an additional identification tool which could work as follows: for example, an identification card provided with a chip could broadcast the identity of the individual to the identification unit, which would proceed to compare the template associated to the identity of the individual with the biometric data presented to it at this particular moment.

In the case in point, the JRC biometric access control system uses a "comparison one to many" search mode. In particular, identification units will compare the fingerprints of the individual with the templates stored in each of the readers in order to ascertain if they match.

As a principle, the EDPS strongly favours the use of "one to one" search mode whereby the identification unit would compare the fingerprints of the individual with a unique template (associated to the identity). As pointed out above, such a search mode system provides more accurate results.

The EDPS understands that in this case, taking into account the limited number of templates, the possibility of errors is very narrow; however, as a matter of principle, the EDPS considers that the "one to one" search mode not only provides more accurate information, it also entails

[5] For a description of the data protection principles applicable in relation to fall back procedures, see Opinion of 13 October 2006 on the draft Council Regulation (EC) lying down the form of the laissez-passer to be issued to members and servants of the institutions, OJ C 313, 20.12.2006, p. 36.

less processing of data insofar as the system only has to match two sets of information pertaining to the same individual (as opposed to matching one set of information against the templates of many individuals). Hence, this search mode is inherently less privacy invasive.

In selecting "one to one" search mode, the EDPS recommends to use systems that store the biometric templates in chips rather than in central databases, or in this case, in various reader systems. The storage in chips is obviously more privacy friendly insofar as the template is stored on a medium (e.g. badge with chip) which is in the possession of the respective data subject. Thus, the data subject him/herself has the direct control and responsibility of his/her template. No one else has access nor is in possession of his/her template. An additional problem with the storage in databases is that it triggers the risk of so-called "fishing expeditions", accessing the database for purposes different from those for which the database has been conceived. A decentralized system solves this risk without eroding the security level.

On the basis of the reasons described above, the EDPS considers that the existing JRC access control system using biometric data should be changed, if necessary progressively. The EDPS envisages that in a first phase, JRC could introduce a "one to one" search mode by introducing an additional identification, for example, in cards used for standard access control systems. This could be achieved by upgrading the existing access control with device-embedded SmartCard readers which would identify the individual in the database.

At a later stage, the EDPS wants to see a complete change in the search mode, a move to the "one to one" search mode where biometrics would be stored in chips rather than in a central database/individual biometric readers. The EDPS calls upon the JRC to consider updating the system taking into account the recommendations outlined above. In doing so, it would be advisable to conduct an impact assessment. Finally, the EDPS calls upon the JRC to present a viable timetable to implement these changes.

The solution to which the EDPS is aiming at is currently being developed by DG HR DS of the European Commission in its access control project (PACS), where the use of biometric data is coupled with the used of a protected chip embedded in the staff badge.

### 2.2.5. Conservation of data

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that "*personal data must be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they were further processed". "The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted".*

Access Control System transactions and anomaly data have only been kept since 2002 in its present format. Being complimentary to daily permit, staff pass and special authorisation related information, the data controller considers that it should be kept for at least 12 years.

The data controller also stated that after the standard retention period of 12 years, data related to general access control transactions will be anonymised in order to be able to produce statistics.

For what concerns the registration of controlled zones or nuclear areas entry/exit, the duration of the retention period is 30 years due to legal requirements e.g. to store Dosimeter assignments for health reasons.

The EDPS does not share the view of the JRC that the access control data transactions (logs) and anomaly data have to be kept for at least 12 years.

The EDPS considers that timing is a key element in the discovery of security incidents. Indeed, the more sensitive a system is, the earlier the detection of security incidents has to take place. The EDPS understands that it may be necessary to keep an audit trail of the registering data for a period of time which allows reconstructing events during security related incidents and that in the case of the JRC, it may not be practical to have a very short period. The EDPS assumes that the JRC has in place or, if not, should develop a process of identifying and responding to incidents so that they are detected and reported as soon as possible after they have occurred. Presumably the JRC aims at discovering incidents immediately after they take place and in any case no later than several months thereafter.

Based on the foregoing, the EDPS considers that the period of 12 years is clearly excessive and invites the JRC to reconsider the setting of its conservation period for transactions and anomaly by reassessing the need to shorten this time by using the statistics of incidents.

The fact that this period should be linked to the rules of 12 years on site is not justified, because the data from the access control system are not designed to be used for ensuring that a person fulfils the 12 years rule imposed on JRC sites.

As regards the time limit to block/erase data on justified legitimate request from the data subjects, this is performed through SECPAC and ARDOS and therefore follows the procedure established in these processing operations.

Finally, as regards the production of anonymous statistics on personal data performed after the retention period. It is important that such anonymisation complies with Article 4(1)(e) of the Regulation. Therefore, the JRC should clarify to the EDPS the procedure it will use for the anonymisation of the data.

### 2.2.6. Transfer of data

According to the notification and the privacy statement, services within the JRC, DG HR/DS or national law enforcement agencies may receive the data.

The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data be transferred if it is "*necessary for the legitimate performance of tasks covered by the competence of the recipient"*. In order to comply with this provision, in sending personal data, the Security service of the JRC must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. Whether a given transfer meets such requirements will have to be assessed on a case by case basis. In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.

Regarding the disclosure to national law enforcement agencies, in case of crime prevention or investigations, the JRC foresees a procedure requiring a written request by national authorities and that the transfer be duly authorized by the controller. In such case, the EDPS underlines that Article 8 of Regulation (EC) No 45/2001 requires that personal data shall only be transferred if *"(a) the recipient establishes that the data are necessary for the performance of*

*a task carried out in the public interest or subject to the exercise of public authority, or (b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"*. In the cases foreseen, Article 8 would be complied with by the JRC.

The EDPS also notes that the JRC stated that for contractual invoicing reasons, the data on real presence (in connection with SECPAC) on site of staff working for external contractors could be transferred to all Management Support Units (MSU) on the Ispra site. The EDPS considers that such processing does not fall within the purposes of access control processing operations. Indeed, the data on real presence are not part of the access control purpose, as described in the notification. Therefore, the EDPS invites the JRC to notify separately the procedure relating to external contractors, unless this practice is discontinued as announced in the comments of the data controller to the draft opinion. In such case, it should be clearly stated in the follow-up.

**2.2.7. Right of access and rectification**

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

The prior checking notification and the supplementary information submitted by the controller (privacy statement) describe the possibility of access to and mention the possibility of rectification of personal data by a staff member. The privacy statement which was submitted to the EDPS for review provides the name of the person responsible for the execution of these rights. It also foresees that upon justified request from the Data Subject data will be modified, frozen or eventually erased in a maximum period of one month.

The EDPS recalls that these rights apply not only to the information provided by the individual (identification information and fingerprint templates) but also to the information generated every time an individual accesses a the secured zones.

Should Article 20 be applied, the EDPS reminds the JRC that it should be applied restrictively and on a case by case basis.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met.

**2.2.8. Information to the data subject**

Articles 11 and 12 of Regulation (EC) 45/2001 list information that must be provided to the data subjects.

Data subjects are informed by a "privacy statement Access Control System at JRC Ispra". This privacy statement is relevant for the general access control system and as such complies with Article 11 and 12 of the Regulation.

However, this privacy statement does not cover the specificities of the biometric enrolment. As stated by the data controller: "*As such readers are used only by a very limited number of*

*staff, with respect to the rest of the Access Control System, they have not been explicitly mentioned in the Privacy Statement. Users are informed verbally during the enrolment process about the type of data stored*".

The EDPS does not consider sufficient to inform verbally the staff members who will be enrolled, using biometric data. A specific privacy statement should be provided to individuals who undergo an enrolment phase and should, besides the information provided in the general privacy statement, also contain the following:

- The purpose of the processing operation using biometric data
- Mention whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply (for instance, the consequences of failure to enrol). By analogy with a questionnaire, the staff should be informed of the practical consequences to enrol and of failure to do so;
- The existence of a fallback procedure
- The storage period of the logs of access.

In another prior-checking analysis[6], the EDPS acknowledged the procedure implemented at the European Central Bank at the time of enrolment (i.e. "*the privacy statement will be provided* [o]*n paper and individuals will be asked to sign it stating that they have read and understood the statement*"). The EDPS considers that this is an appropriate method of providing the information and suggests that a copy of the privacy statement be given to individuals so that they can go back to the privacy statement in case, for example, they want to know how to exercise their rights or how the data processing takes place.

### 2.2.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

For those processing operations where the use of fingerprint technology proves to be necessary, the EDPS notes that the technical and organizational measures appear to be suitable in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected.

## 3. Conclusion:

The EDPS considers that the JRC is in breach of the provisions of Regulation 45/2001 in that it did not fulfil its obligations as regards the notification to the EDPS of the processing operation under analysis, but installed and ran the processing before submitting it to prior-check. Due to the delicate nature of the case, which involves biometric data, it was particularly crucial that the prior checking assessment was conducted *ex ante*.

Furthermore, as regards other aspects of the processing operation, the EDPS considers that the JRC should:

[6] See Opinion on the European Central Bank access control (2007-501).

- Comply with the EDPS Videosurveillance Guidelines, as regards the use of video-surveillance cameras at the JRC Ispra;

- Consider enacting a legal instrument providing the legal basis for the processing operations that take place in order to set up an access control system based on the use of biometrics (fingerprint);

- Provide the EDPS with the FRR established by the Security Service Contractor as well as the operational FRR, which is effectively used;

- Reconsider the decision taken in terms of technological choices through an impact assessment, including a viable timetable to implement changes in technology, i.e. in the current fingerprint system. In a first phase, consider introducing a "one to one" search mode by including an additional identification. At a later stage, consider changing to a "one to one" search mode where biometric data would be stored in chips rather than in various individual readers;

- Reconsider the setting of the conservation period of transactions and anomaly by reassessing the need to shorten this time by using the statistics of incidents;

- Clarify the procedure used for the anonymisation of the data after the end of the retention period;

- Notify the processing operation concerning the external contractors, unless this procedure is discontinued. In such case, this should be specified in the follow-up;

- Adopt a specific privacy statement regarding the processing of biometric data, as recommended in this Opinion and ensure that a copy of the privacy statement is given to individuals or that it is made available to them in a way that allows them to consult it.

Done at Brussels, 15 July 2011

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor