Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank related to the extension of a pre-existing access control system by an iris scan technology for high secure business areas

Brussels, 14 February 2008 (Case 2007-501)

1. Proceedings

On 3 September 2007, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of the European Central Bank ("ECB") a notification for prior checking ("the Notification") regarding the data processing operations relating to the operation of an iris scan technology system implemented into a pre-existing contactless badge reader based access control system.

On 25 and 28 September 2007, the EDPS made requests for additional information, which the ECB Data Protection Officer ("DPO") answered together on 16 November 2007. On 6 December 2007, the EDPS requested clarification of some of the ECB responses related to technical aspects of the iris scan technology. The DPO of the ECB provided the explanations on 22 January 2008. On 1 February 2008, the EDPS sent the draft Opinion to the Data Protection Officer ("DPO") of the ECB for comments which were received on 7 February 2008.

2. Examination of the matter

2.1. The facts

The ECB has set up an access control system which, among others, scans the iris of ECB staff members and external individuals (hereinafter "staff members" or "individuals") accessing highly secured areas within the ECB. The data generated by the access control system are also used to reconstruct events during security related incidents.

The overall ***purpose of the data processing*** is twofold; on the one hand the access control system is used to control the access to highly secured areas within the ECB. In addition, it is also used to reconstruct events during security related incidents.

The primary ***responsibility for the data processing*** lies within the Directorate General Administration, in particular within the Security Division, a sub-unit of which, the Security Service Centre, carries out all the data processing operations.

The ***manual and automated data processing*** operations are closely interrelated and can be described in a combined fashion as follows:

In order to operate the access control system, individuals who need to access highly secured areas go through an *enrolment procedure*. As a part of this procedure, the Security Service

Centre takes biometric iris templates of both eyes. Additional information that is collected at this stage includes the name of the individual, his/her personnel number (if applicable) and the business unit to which he/she is attached. The details mentioned before and the iris templates are stored in a separate server located within the ECB premises (technical room Security Division), from which the key identification data are transferred to relevant identification units. These units are located at the transition points to selected highly secured zones, i.e. security locks in front of computer centre areas and in front of the sensitive Banknotes area. The request forms for the access rights are scanned and stored on the Security Service Centre network drive.

Additional data processing occurs at the moment when individuals wish to access the highly secured areas controlled by the iris control system. In order to be able to access the highly secured areas and in addition to the standard access control system, individuals have to be validated by an identification unit. In doing so, the unit will compare the iris of the individual with all templates in order to ascertain if they match. If they do, they will be able to enter the given zone. In addition, the access control system will log the time of access.

Data subjects involved in the processing are *(i)* selected ECB Staff members and *(ii)* consultants and subcontractors who need to access the highly secured areas within the ECB premises.

The ***categories of personal data*** collected include the name, personnel number, business unit, biometric eye templates of both eyes, and the time when the individual accessed (or tried to access) the security areas controlled by the system. The number of people whose data will be processed is close to four hundred out of 4500 data files of individuals with temporary or permanent access rights to ECB premises. This number is subject to a frequent reconciliation process performed on a case by case and 'need-to-have' assessment.

As far as ***conservation of data*** is concerned, all the above information will be retained for the period of time that the data subject has an employment contract or is otherwise engaged with the ECB until three months after expiry or termination of the employment contract or other engagement. The data generated when individuals access/try to access highly secured areas are stored for security purposes for a limited period not exceeding one year.

Personal data are not ***transferred*** outside the ECB. The information generated when individuals access/try to access highly secured areas may be transferred within the Security Division in the context of administrative inquiries to reconfirm logged data of the access control system. However this has never occurred yet.

As far as the ***right to information*** is concerned, individuals are provided a paper privacy statement which informs them of the purpose of the processing, the existence of a right of access and rectification, the possibility of recourse to the European Data Protection Supervisor and the retention periods. The DPO sent a copy of the information notice to the EDPS by e-mail of 25 September 2007.

The right of access and rectification are recognized. The privacy statement also indicates the person responsible for the execution of these rights.

Security measures are implemented.

2.2. Legal aspects

2.2.1. Prior checking

This Prior check Opinion relates to processing of personal information carried out by the ECB, in particular the Security Division to control the access to highly secured areas within the ECB and reconstruct events during security related incidents.

Applicability of the Regulation. Regulation (EC) No 45/2001[1] applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*"[2]. For the reasons described below, all elements that trigger the application of the Regulation are present:

First, *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed. Second, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001, as well as manual data processing operations. Indeed, the personal data such as iris templates of both eyes are collected in various chronological stages and undergo 'automatic processing', for example when the Security Service Centre takes the templates of both eyes as well as for each validation, i.e. when the individual accesses the highly secured areas. Finally, the processing is carried out by a Community body, in this case by the European Central Bank, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

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 considers that the presence of some biometric data other than photographs alone, such as the case in point where biometric eye templates of both eyes are collected, presents specific risks to the rights and freedoms of data subjects. These views are mainly based on the nature of biometric data which is highly sensitive, due to some inherent characteristics of this type of data. For example, 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 the highly sensitive nature of the data, 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.

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 operations have already been established. This is not an insurmountable problem provided that all recommendations made by the EDPS are fully taken into account and the processing operations are adjusted accordingly.

---

1 Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ("Regulation (EC) No 45/2001").
2 See Article 3 of Regulation (EC) No 45/2001.

Notification and due date for the EDPS Opinion. The Notification was received on 3 September 2007. 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 99 days to obtain additional information plus 6 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later 18 February 2008 (17 February being Sunday).

2.2.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. As pointed out in the Notification, the grounds that justify the processing operation are based on Article 5(a), pursuant to which personal data may be processed if the processing is "*necessary for the 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*". In order to determine whether the processing operations in question comply with Article 5(a) of Regulation (EC) No 45/2001 two elements must be taken into account: First, whether either the Treaty or other legal instruments foresee a public interest task that entails the processing of personal data (legal basis), and second, whether the processing operations are indeed necessary for the performance of that task (necessity test).

As far as the legal basis is concerned, the DPO of the ECB informed the EDPS that the ECB considered that the setting up of an access control system with iris scanning capabilities fell within the competence of the Executive Board on the basis of Article 11.6 of the Statute of the European System of Central Banks and of the European Central Bank ("Statute"). Article 11.6 establishes that "*The Executive Board shall be responsible for the current business of the ECB*". The setting up of an access control system based on the use of biometrics is therefore considered as "current business" and as such does not require a specific legal basis. How the setting up of an access control system is legally formulated is of course a matter for the ECB. However, the EDPS questions whether this approach is adequate and believes that it would be more appropriate for the ECB to adopt another more specific legal basis foreseeing the processing operations at stake. In this regard, the EDPS notes that Article 11 of the Rules of Procedure of the European Central Bank entrusts the Executive Board to enact organizational rules referred to as administrative circulars which are binding on the staff of the ECB. Thus, organizational rules affecting the ECB must be adopted through administrative circulars. The setting up of an access control system is a measure that relates to the organization of the ECB, and in its view is necessary in order to optimize the security and overall functioning of the ECB. This is even more relevant if one takes into account that this measure will affect a fair number of the staff working for the ECB. Based on the foregoing, it appears that the setting up of an access control system based on iris scan technology should be carried out pursuant to an administrative circular. For this reason, the EDPS calls upon the ECB to reconsider the legal basis for the setting up of such system.

As to the necessity of the processing (*necessity test*), the EDPS takes note that the ECB safeguards important monetary policy, financial and economic information. Taking into account the relevance of these interests and in order to prevent the unauthorized access and disclosure of this information, the ECB could indeed find it necessary to adopt special security measures, including the setting up of stringent access control systems for specific areas of the ECB. Therefore, in the EDPS' view, the implementation of strong access control systems which entail the processing of personal data can in this case reasonably be considered as a necessary internal control measure towards the safeguard of monetary policy, financial and economic information.

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.

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 involves mainly the processing of biometric data, is in line with this principle, the EDPS notes the following:

The type of data collected, mainly the iris templates of both eyes and related identification information, corresponds to the data required to operate an access control system based on biometrics. From this point of view, the data collected are adequate and relevant for the purposes of the processing. The ECB informed the EDPS that previous to the selection of the iris scan technology, the use of biometric ID systems at the EBC was laid down in a document ("ECB Physical Security Guide") which constituted the basis for selecting the iris scan technology. Among others, the document compared different biometric systems and highlighted the advantages and disadvantages of each of them. Part of the analysis included, although somehow marginally, some data protection / privacy related issues. Additional documents were also used to make the choice. The EDPS welcomes this practice. Taking into account the highly sensitive nature of the biometric data in order 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 justified the use of such technique and whether other, less privacy intrusive alternatives, were envisaged. Vis-à-vis the future and particularly concerning possible updates of the system (see below under "Accuracy"), the ECB should conduct additional targeted impact assessment where privacy/data protection considerations should be more prominently taken into account.

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 biometric data, used for access control purposes. 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 iris. This is usually referred to as

"fall back procedures"[3]. 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***"). If these measures are not embedded in the architecture of the system, the accuracy of the information produced by the system may be compromised. In particular, in the case of false rejection, the system will produce a record that a given individual without proper access rights intended to access a highly secured area, when in fact the individual did have such rights. At the same time, because the individual will be misidentified, he/she will be denied a right (the right to access) to which he/she is entitled. The false rejection rate ("FRR") or likelihood of false rejection depends on the matching threshold set forth by the operator. For example, the operator may decide that only a matching percentage of 95% equals to identification. Presumably, higher percentages will be set up for premises which need higher levels of protection. Also, the higher the percentage, the more often it will trigger false rejections.

As to alternative ways to identify individuals who are not eligible for enrolment, the ECB has informed the EDPS that it has foreseen a fall back procedure called "remote access procedure", further described below, that can be used in such cases.

As to the measures to deal with false rejections, the EDPS has been informed that the ECB has considered all the factors that may increase false rejections and its impact mitigated to the utmost. As outlined above, the ECB has also informed the EDPS that in setting up the access control system it has foreseen a fall back procedure that can be used when individuals are misidentified and thus their access to highly secured zones denied. The fall back procedures envisaged involve a remote entry process including standard access control identification and remote video surveillance verification by ECB Security. This procedure seems appropriate insofar as it addresses the problem in a way that does not put too much burden upon individuals. In other words, the alternative procedures provide sufficiently simple solutions to the problem of misidentification and rejection. These views are further supported in the light of the limited number of individuals concerned and small probability of misidentification.

Second, 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 ECB access control system uses a "comparison one to many" search mode. In particular, identification units located at the transition points to selected highly secured zones will compare the iris of the individual with all templates previously stored in a database in order to ascertain if they match. In principle, the EDPS favors the use of "one to one" search mode whereby the identification unit would compare the iris of the individual

[3] 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) laying 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.

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 (approximately 400) the possibility of errors is very narrow; however, as a matter of principle, he favors the use of "one to one". The "one to one" search mode not only provide more accurate information, it also entails 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 prefers systems that store the biometric templates in chips rather than in central databases. 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 central 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.

The EDPS understands that in 2002 the iris identification system needed to be integrated into a pre-existing access-control system, which did not allow the one to one search mode. At that stage the existing access control system was not capable of implementing the iris scan system into the existing infrastructure. As a consequence, those considerations have made it difficult for the ECB to implement a "one to one" search mode. However, because of the reasons described above, the EDPS considers that the existing ECB access control system should be progressively changed. The ECB has recognized the positive advantages of the "one to one" search mode and said that in the future it will switch to such a search system. The EDPS envisages that in a first phase, the ECB could introduce a "one to one" search mode by introducing an additional identification, for example, in cards used for standard access control systems. As explained above, this could be achieved by upgrading the IrisAccess 4000 with device-embedded SmartCard readers which would identify the individual in the database. According to the provider, IrisAccess 4000 has the ability to function with HID iCLASS, DESFire, and MiFARE and CAC-compliant cards. One of these standards might correspond to the one used by the standard ECB access badge. Alternatively, a chip corresponding to one of these standards could also be embedded in the ECB access badge.

At a later stage, the EDPS would like 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. The EDPS calls upon the ECB to consider updating the system taking into account the suggestions outlined above. In doing so, it would be advisable to conduct an impact assessment. Finally, the EDPS calls upon the ECB to present a viable timetable to implement these changes.

2.2.5. Conservation of data

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed. This is usually referred to as 'conservation principle'.

According to the Notification, the iris scan templates and identification information will be retained for the period of time during which the staff member has an employment contract or

is otherwise engaged with the ECB until three months after expiry or termination of the employment contract or other engagement. The EDPS considers this retention period as appropriate insofar as the data kept are necessary during all the time that the individual has an employment relationship with the ECB which requires him/her to access ECB's highly secured areas.

The ECB also stores files that reveal whenever an individual accessed or tried to access the highly secured areas controlled by the system. The ECB has justified on security grounds the need to keep such information for one year. The EDPS understands that it may be necessary to keep an audit trail of the registering data for a period of time in order to reconstruct events during security related incidents. However, it seems unlikely that audit trail data that go back one year will be of any use. Timing is a key element in the discovery of security incidents. The EDPS assumes that the ECB has in place a process of identifying and responding to incidents so that incidents are detected and reported as soon as possible after they have occurred. Presumably the ECB aims at discovering incidents immediately after they took place and in any case no later than a couple of months after they occurred. It seems highly unlikely that a relevant security incident would go unnoticed for twelve months. Based on the foregoing, the EDPS considers that the retention period of audit trail data should be dramatically shortened. The storage period should be determined by the time it usually takes for the ECB to discover a security incident from the moment that it took place. The EDPS considers that it is unlikely for this to take twelve months and considers that a one/three month period should be sufficient.

2.2.6. Transfers of data

According to the facts, information may be transferred within the ECB in case of security inquiries, but in no circumstances will the data be transferred outside the ECB. Accordingly, Articles 7 of Regulation (EC) No 45/2001 which sets forth certain obligations applying when data controllers transfer personal data to Community institutions or bodies will apply.

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 Division 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.

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.

According to the Notification and information notice, the rights of access and rectification are recognized. The privacy statement provides the name of the person responsible for the execution of these rights. The EDPS recalls that these rights apply not only to the information

provided by the individual (identification information and iris templates) but also to the information generated every time an individual accesses a highly secured zone. .

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

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

In order to show compliance with these articles, a copy of a privacy statement was provided to the EDPS. The privacy statement is supposed to be provided to individuals who undergo an enrolment phase in order to access the ECB highly secured areas. The privacy statement will be provided in 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 suggest that a copy of the privacy statement to 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.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001. The privacy statement contains information on the purposes of the processing and how the data are processed, the conditions for the exercise of the right of access and rectification, the time limits for storing the data and the possibility to have recourse to the EDPS. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation, however, he considers that several amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

(i) The identity of the data controller (the Security Division) should be added.
(ii) In order to ensure full transparency and fair processing, it would be appropriate to add a contact address (that of the data controller or someone from his Unit) where staff members could send questions regarding the privacy statement.
(iii) It would be appropriate to indicate that, if necessary, the information may be transferred for the purposes of carrying out an administrative inquiry.

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. 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

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, the Security Division must:

- 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 (iris scan);
- 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 iris scan system. In a first phase, consider introducing a "one to one" search mode by including an additional identification, for example, using ECB standard access badges together with the upgraded IrisAccess 4000. At a later stage, consider changing to a "one to one" search mode where biometric data would be stored in chips rather than in a central database;
- Shorten the deadline for the storage of audit trail data which reveals whether an individual accessed or tried to access the areas controlled by the system;
- If in the future data transfers take place, ensure that notices are sent to Community institutions receiving data processed in the context of the iris scan system informing that the personal data can only be processed for the purposes for which they were transmitted;
- Amend the privacy statement as recommended in this Opinion;
- 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, 14 February 2008

Peter HUSTINX
European Data Protection Supervisor