



## **Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank related to the application of the security clearance rules**

Brussels, 7 September 2007 (Case 2007-371)

### **1. Proceedings**

On 4 June 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 related to the application of the security clearance rules.

The EDPS requested complementary information on 19 July 2007. The information was provided on 25 July 2007. On 1st August 2007 the EDPS sent the draft Opinion to the Data Protection Officer ("DPO") of the ECB for comments which were received on 28 August 2007.

### **2. Examination of the matter**

#### **2.1. The facts**

This prior check concerns the data processing activities which the ECB carries out in order to run security clearance procedures on (i) candidates selected for employment at the ECB, (ii) non-staff members and (iii) unescorted visitors who have to move within the premises of the ECB. Towards this end, the ECB collects and further processes the legal/criminal history related to these three categories of individuals. The information is provided mainly through a self-declaration submitted by the data subject or in the certificate of good conduct. Individuals that have not committed offenses as reflected in the certificate of good conduct and who have answered negative to various questions in the self-declaration will be issued a security clearance. In other cases, a Panel will review the file and make a recommendation as to whether a security clearance should be issued or not.

The overall *purpose of the data processing* is to determine whether or not a person is eligible for a security clearance. The primary *responsibility for the data processing* lies within the Directorate General Administration, in particular within the Security Division ("A/SET") who carries out all the data processing operations.

As further described below, the *manual and automated data processing* operations are closely interrelated and can be described in a combined fashion as follows: the Head of A/SET keeps a security file for (i) each candidate selected for employment at the ECB, (ii) non-staff members and (iii) unescorted visitors who have to move within the premises of the ECB carried out by the ECB. The security file is paper based. The information contained in the security file can be summarized as follows:

Firstly, the file contains a self declaration form which has been completed by each individual of the categories (i) and (ii) described above in paper form and it is later on provided to the Head of

---

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail: [edps@edps.europa.eu](mailto:edps@edps.europa.eu) - Website: [www.edps.europa.eu](http://www.edps.europa.eu)

Tel.: 02-283 19 00 - Fax : 02-283 19 50

A/SET. Applicants applying for employment at the ECB fill in the self-declaration form on-line, using the e-recruitment tool "Working for Europe", which is then sent to a dedicated e-mail address if any of the questions in the self-declaration applies to them. Selected staff members of the A/SET will store such mails and have access to them for a period of time. A print-out of the form is included in the security file only once the candidates have been selected for employment at the ECB.

In addition, in most cases the security file will contain a certificate of good conduct ("certificate")<sup>1</sup>. If the certificate shows the absence of offences and the responses in the self-declaration are answered in negative, a security clearance will be issued. Otherwise, a Panel will review the file and make recommendations to the Director General of Human Resources, Budget and Organization or (in specific cases) the Executive Board. Individuals will be informed. All the correspondence and the Recommendation of the Panel will be included in the security file. In those cases where a certificate is not necessary, the Panel will examine the matter taking into account what is stated in the self certification.

**Data subjects** involved in the processing are (i) applicants applying for employment at the ECB, (ii) non-staff members, and (iii) unescorted visitors who have to move within the premises of the ECB. In addition to the above, other data subjects whose information is also processed include members of the Panel.

The **categories of personal data** collected include the identification and contact information of each data subject and the legal/criminal history related to this person. Such information will be provided through the self-declaration submitted by the data subject or in the certificate of good conduct, issued by a competent national security authority of an EU Member State at the request of the individual. In addition, other related data will include the recommendation of the Panel and the decision of the respective Director General (when applicable), and a copy of the security clearance form.

As far as **conservation of data** is concerned, the paper file will be kept for the period of time that the data subject has an employment contract or is otherwise engaged with the ECB until one year after expiry or termination of the employment contract or other engagement. If the contracts have a shorter duration, the minimum time that the file will be kept is three years. Data files of unescorted visitors will be kept for a period of one year after the data subject's last date of access to the ECB. After the retention period, the security clearance file is permanently destroyed.

The on-line self declaration forms referred to above are deleted from the Outlook application once the process of recruitment and the issuing of a security clearance have been finalized. The electronic data in the dedicated e-mail address will be kept until six months after the recruitment period in order to accommodate for the situation that DG-Human resources may use data of reserve candidates to fill similar or other suitable positions. At this point, after six months, only the paper based file will exist.

Personal data are not **transferred** outside the ECB. The information may be transferred within the ECB in the context of administrative inquiries. Pursuant to the Administrative Circular (AC) on Administrative Inquiries adopted by the Executive Board of the ECB<sup>2</sup>, the Executive Board

---

<sup>1</sup> The ECB Draft Administrative Circular on Security Clearance Rules defines the Certificate of good conduct as follows: "Certificate issued by a national or local competent authority of the State of residence of the data subject that specifies whether or not he/she is of good conduct, i.e., a certificate that lists - in accordance with the relevant national or local laws - the criminal offences for which the individual has been convicted "

<sup>2</sup> The data processing that takes place in the context of carrying out administrative inquiries has been prior checked by the EDPS, see: Opinion of 8 March 2006 on a notification for prior checking on "Disciplinary cases (including related administrative reviews of complaints and grievances, Ombudsman and Court cases)" (Case 2004-270).

('EB") may decide to open an administrative inquiry and nominate a lead inquirer, meaning a senior manager of the ECB. The lead inquirer organizes the administrative inquiry and may appoint a Panel to investigate any breach of professional duties. The composition of this Panel (not more than 5 persons) may include persons from various business areas, depending on the expertise needed. The personal data stored in the security clearance file may be transferred to members of this Panel if deemed necessary.

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 statement also refers to potential transfers of the information within the ECB to authorised staff. Individuals are asked to sign the letter acknowledging that they have read it and understood it. **The right of access and rectification** are recognised with an indication of 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 the collection and further processing of personal information carried out by the ECB to support the ECB's decision, for applicants, ECB Staff and ECB unescorted visitors, to issue or not security clearance.

The procedures that the ECB follows in order to determine whether individuals are eligible for a security clearance are reflected in a Draft ECB Administrative Circular, which the ECB aims to adopt in 2007.

**Applicability of the Regulation.** Regulation (EC) No 45/2001 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*"<sup>3</sup>. 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 in order to determine whether individuals are eligible for security clearances. 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 information is first collected both on paper and electronically and is then stored in a paper security clearance file. 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*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (a), the processing of data relating to "*suspected offences, offences, criminal convictions or security measures*". This type of information is collected to enable the ECB to assess the reliability of

---

3 See Article 3 of Regulation (EC) No 45/2001.

individuals in order to decide whether or not a security clearance should be issued. Therefore the processing operations must be prior checked by the EDPS.

***Notification and due date for the EDPS Opinion.*** The Notification was received on 4 June 2007 March 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 33 days. The Opinion must therefore be adopted no later than 10 September 2007.

## **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 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).

In ascertaining the legal grounds in the Treaty or other legal instruments that legitimise the processing operations (*legal basis*), including the collection of information about criminal convictions in the context of running security clearance procedures, the EDPS takes note of the following: First, the information provided by the DPO of the ECB regarding the following amendments of the Conditions of Employment of the ECB. Indeed in order to introduce a security clearance procedure, the Conditions of Employment of the ECB (as well as the Conditions of Short-Term Employment) need to be amended. Such amendment requires the consultation of the ECB Staff Committee, which the Directorate General of Human Resources, Budget and Organization has commenced by letter of 8 June 2007. The consultations of the Staff Committee and the prior check notification to the EDPS have been executed in parallel in order to ensure that all relevant input to the procedure is available in time. The draft Decision inserts a legal basis into the Conditions of Employment of the ECB and the Conditions of Short-Term Employment, which reads as follows:

### ***Article 1 Medical and Security Clearance***

The following paragraph shall be inserted as Article 4. (g) of the Conditions of Employment:

4. (g) Employment with the ECB is subject to medical and security clearance.'

### ***Article 2 Security Clearance***

2.1 The following Article shall be inserted as Article 10 of the Conditions of Short-Term Employment:

10. Employment with the ECB is subject to security clearance.

Of course, pending the outcome of the Staff Committee consultation the wording of the legal provisions may change.

Second, the draft ECB Administrative Circular XX/2007 on Security Clearance Rules set forth the procedures for running security clearance checks upon staff members and selected candidates as well as non-staff members and unescorted visitors. Among others, the Circular expressly foresees the collection of the self-declaration form and the certificate of good conduct and foresees their storage in a personal security file. The Administrative Circular sets forth the purpose of the data processing, as well as the procedures and responsibilities of the various actors within the ECB in the context of the implementation of the security clearance rules, including the

collection of the documents and their examination, depending on whether the security clearance must be carried out regarding a staff member and selected candidates or to non-staff member and unescorted visitors. In addition, the Administrative Circular sets forth the conditions and conservation time of the security clearance file.

Clearly, the data processing operations notified for prior checking take place on the basis of this legal framework which foresees not only the collection of the data but most of the aspects of the data processing. For the time being, the legal framework, both the Conditions of Employment of the ECB and the draft ECB Administrative Circular XX/2007 are still in draft form. In order for the processing to be properly based on this legal framework they must be formally adopted.

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 unauthorised disclosure of this information, it appears necessary for the ECB to adopt special security measures, not only vis-à-vis external threats but also vis-à-vis internal risks. The running of security clearance seems to be an internal control measure towards minimising the safeguard of monetary policy, financial and economic information. Among others, such internal controls aim at preventing the access to the ECB premises of those individuals who, in the light of their background, particularly criminal history, may constitute a threat to the ECB. By the same token, in order to minimise the risk, it is important for the bank to hire only individuals whose criminal history does not question their capacity to maintain high standards of professional ethics in the performance of their duties at the ECB. In order to filter individuals who may not be up to such standards or whose mere presence in the ECB premises may pose a threat to the ECB, it seems necessary to collect and further process personal data that reveal the criminal history of such individuals. Indeed, unless A/SET collects and further processes personal information of the nature listed above, it will not be able to determine whether an individual is sufficiently trustworthy and reliable to be allowed unescorted in the ECB premises.

### **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 data processing obviously includes data relating to criminal offences and pending investigations, which is regulated under Article 10.5 of Regulation (EC) No 45/2001. For example, in many instances individuals have to provide a certificate of good conduct and in all cases, they have to fill in a self clearance declaration form which includes questions as to whether they have been convicted, fined or imprisoned for infringing any law (excluding minor traffic offences). It also asks whether there are criminal cases pending or whether individuals have been subject to an investigation for a criminal offence. In addition, the self declaration form requires individuals to provide information related to offences (whether the individual has been declared bankrupt or there has been a petition for bankruptcy in the last 10 years and whether the individual can fulfil his/her financial obligations).

In this regard, the EDPS recalls the application of Article 10.5 of Regulation (EC) No 45/2001 which establishes that "*[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor.*" In the present case, processing of the mentioned data is expressly authorised by the legal instruments mentioned in point 2.2.2 above, once they are formally adopted.

### **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 analysing whether the processing at point, which involves mainly the processing of data related to offences or criminal convictions, is in line with this principle, the EDPS notes the following:

First, the ECB Draft Administrative Circular on Security Clearance Rules foresees the collection of a record that compiles an individual's criminal convictions and foresees its storage in a personal security file. In legal terms this is referred to as 'criminal record'. However, oddly the ECB Draft Administrative Circular on Security Clearance Rules does not use the appropriate legal nomenclature referred above, i.e., "criminal record". Instead, the ECB Draft Administrative Circular on Security Clearance Rules explicitly refers to a "certificate of good conduct", yet it defines it as a criminal record<sup>4</sup>. In legal terms and particularly in certain Member States, certificates of good conduct contain information that goes beyond a record containing criminal convictions. In particular, in some Member States a certificate of good conduct may contain information about the character of an individual, his moral behaviour, etc. Whereas, as discussed above, it appears necessary for the ECB to collect information contained in criminal records in order to filter individuals that may pose a risk to the ECB, it does not appear necessary to have the information that may be contained in a certificate of good conduct.

The EDPS understands that the ECB does not intend to process information on the character of an individual or his moral behaviour that goes beyond this. However, this may happen as a result of the use of the nomenclature "certificate of good conduct". For this reason, the EDPS is of the view that it may be preferable in the ECB Draft Administrative Circular on Security Clearance Rules to redefine the nomenclature and its definition in order to prevent the collection of information that goes beyond the recollection of criminal convictions (such as information about the character of an individual, his moral behaviour).

Second, the self declaration includes a first question which reads as follows: "*Have you ever been convicted, imprisoned, fined for infringing any law (excluding minor traffic offences) in any country?*" Two options are given: "yes" or "no". Should the answer be "yes", the candidate is requested to give details on the conviction(s), the fines and imprisonments. Convictions for minor traffic offences are excluded. For the two reasons described below, the EDPS considers that this question should be re-phrased:

(i) The EDPS notes that fines and imprisonments are two types of punishments that may be imposed as a result of a conviction. It is appropriate for the ECB to collect information about convictions and also about the type of punishment that was imposed as a result of a conviction as this information may show the gravity of the conviction and may be useful in order to filter individuals who may pose a risk to the ECB. However, the reference to "imprisonments" may be understood to include imprisonments of preventive nature that have not lead to a criminal conviction, because the individual was deemed not guilty, and yet the individual had been subject to preventive imprisonment. Taking into account that the purpose of the data processing is to filter individuals that may pose a risk to the ECB, the collection of information that reveals that an individual was imprisoned and then deemed not guilty seems excessive. Accordingly, the EDPS considers that the reference to the "*imprisonment*" in the first question should be re-phrased. For example, the sentence could be drafted as follows: "*Have you ever been convicted for infringing any law (excluding minor traffic offences) in any country? If so, provide details regarding the nature of the*

---

<sup>4</sup> See footnote (x) above which reproduces the definition of "certificate of good conduct" contained in the ECB Draft Administrative Circular on Security Clearance Rules.

*conviction and the punishment (imprisonment, fine, etc.).”* In this way, the answers will be linked uniquely to imprisonments that are the result of a conviction.

The above remark is further reinforced if one takes into account that the second question in the self-declaration form asks individuals whether there are any criminal pending cases. Thus, if an individual has been imprisoned preventively and his/her criminal case has not been judged yet, he/she will have to declare the existence of the pending case under the second question. Therefore, this second question covers the eventuality where there is a risk of an individual to be found guilty and he may indeed have been imprisoned preventively but yet his case has not been decided by court.

(ii) The EDPS considers that the first question of the self-declaration presents another related problem. The current phrasing may entice individuals to reveal unnecessary information. In particular, individuals may provide information which goes beyond what would be stated in a criminal certificate. Indeed, after a certain time, which varies for each crime, and may vary country to country, criminal convictions are deemed to be expunged and are deleted from the criminal records. However, the phrasing of the question may result in a situation where individuals will feel obliged to reveal crimes which would no longer be included in a criminal record. The EDPS considers that it would be appropriate to limit the request of information to what it would be included in a criminal record. To this end, the following limitation could be included after the question *"Have you ever been convicted, for infringing any law (excluding minor traffic offences) in any country? If so, provide details regarding the nature of the conviction and the punishment (imprisonment, fine, etc.). Limit your response to convictions whose record delay has not yet expired."*

Third, as stated above, the second question asks if there are criminal cases pending against the individual and or he/she is presently subject to an investigation for a criminal offence in any country. In this case, it also appears appropriate to include the limitation of traffic offences which is included under the first question.

The EDPS calls upon the ECB to amend the self-declaration form following these suggestions.

***Fairness and lawfulness.*** Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 2.2.7.

***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"*. This is usually referred to as 'data quality principle'. In this case, the data include criminal records. In this respect, see discussion under Section 2.2.7.

### **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'.

The EDPS considers appropriate the retention period for data subjects that have an employment contract (until one year after expiry or termination of the employment contract but for a minimum of three years). Indeed, it seems appropriate for the ECB to be able to go back to the

information that constituted the basis for the issuance of the security clearance at any time during the employment contract plus certain additional time. On the other hand, it does not seem appropriate for the ECB to keep information about crimes that have expunged and which would not be reflected any longer in a certificate of good conduct. For this reason, the ECB should find a system whereby information about crimes that has expunged should be deleted. This may be achieved through the right of access and rectification, as described below under 2.2.7.

The conservation time for unescorted visitors also seems as a reasonable period (one year after the data subject last accessed the ECB).

### **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, Article 7 of Regulation (EC) No 45/2001 which sets forth certain obligations that apply 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 "*for the legitimate performance of tasks covered by the competence of the recipient*". Article 11 of the ECB Administrative Circular XX/2007 on Security Clearance Rules also reproduces this rule. In order to comply with this provision, in sending personal data, A/SET 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.

For example, transfers to the Panel to investigate any breach of professional duties will in most cases fulfil the requirement (i) insofar as the Panel will have the appropriate competences to carry out its tasks. However, it will be necessary to assess on a case by case basis whether the transfer of such information to the Panel is necessary in the light of the specificities of the case. Accordingly, A/SET should apply this rule for each particular data transfer. Doing so will avoid unnecessary transfers of information as well as transfers of information. 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<sup>5</sup>.

### **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.

A/SET provides the right of access and rectification to the security clearance files. Individuals are notified of the possibility to exercise such rights and they are given information about whom to contact to exercise these rights. In order to ensure that access requests will be dealt with in a timely fashion and without constraints, it may be appropriate for A/SET to set up reasonable time limits.

The application of the right to rectify inaccurate data may enable individuals to request the update of the certificates of good conduct. Indeed, as noted above under 2.2.5, crimes expunge

---

<sup>5</sup> This issue has been discussed in the EDPS Opinion of 8 March 2006 on a notification for prior checking on "Disciplinary cases (including related administrative reviews of complaints and grievances, Ombudsman and Court cases)" (Case 2004-270).



after certain period of time, and as of this moment, they are not reflected any longer in certificates of good conduct. Under Article 14 of the Regulation individuals have the right to rectify inaccurate or incomplete data, which in the case in point means that individuals should be able to update their certificates of good conduct in order to reflect accurately their current situation. Furthermore, in keeping information about crimes that have expunged the ECB would contravene the data quality principle described above according to which personal data must be "*accurate and, where necessary, kept up to date*".

In order to apply Articles 14, 4(1)(d) and 4(1)(e) of Regulation (EC) No 45/2001 (right of rectification, data quality and conservation principles), the ECB should set up a system intended to ensure the effective application of the content of these rights and principles as far as the certificates of good conduct are concerned.

In setting up this system, the EDPS notes that it may be difficult and cumbersome for the ECB alone operate a scheme that deletes information on crimes that have expunged on its own initiative, particularly because this may depend on country to country. The ECB may not be in a position to verify on on-going bases whether the crimes contained in the certificates of good conduct of each individual have or not expunged. However, the ECB is in a position to inform individuals of the possibility of providing updated certificates of good conduct, throughout their employment relationship with the ECB. Thus, the EDPS calls upon the ECB to remind individuals of such possibility. This can be done in the privacy statement or separately. In providing individuals with this possibility, the ECB is in fact enabling individuals to exercise their right of rectification of data that is inaccurate as recognised under Article 14 of the Regulation. It is also contributing to the application of the data quality principle. Furthermore, it is also implementing the principle that limits the conservation of information when it is no longer necessary for the purposes for which it was processed. In this regard, the EDPS notes that the ECB may need to keep for certain time certificates of good conduct in order to have evidence justifying why it took the decision to issue a negative security clearance. This need may justify the keeping of certificates of good conduct until it is no longer possible to challenge a given negative decision. This should not prevent the individual from providing an updated certificate of good conduct to be kept along side with the former one, which will be definitively deleted after the above mentioned period.

### **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 ensure compliance with these Articles, a copy of a privacy statement was annexed to the Notification. The privacy statement is supposed to be provided to individuals who undergo a security clearance. 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 policy 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, the legal basis for the processing operations 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 (A/SET) 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 EU staff members could send questions regarding the privacy statement.
- (iii) It would be appropriate to indicate that, if necessary, the information may be transferred to the Panels competent to carry out administrative inquiries.

### **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 organisational 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 unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing. The technical and organisational 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 providing the considerations in this Opinion are fully taken into account. In particular, A/SET must:

- Enact legislation as submitted for prior-check providing the legal basis for the processing operations that take place in order to run security clearance procedures.
- Redefine the nomenclature and its definition in order to prevent the collection of information that goes beyond the recollection of criminal convictions
- Include a limit in the first question of the self-declaration form so that individuals are not required to provide information on crimes that would not be included in a criminal record. Also, in this question, delete the reference to imprisonments and consider rephrasing the question as suggested in this Opinion.
- Amend the self-declaration form so that traffic offences are excluded from the scope of the question (which asks whether there are criminal cases pending against the individual).
- Set up reasonable time limits to deal with access requests
- Set up a system to ensure the effective application of the rectification right and data quality and conservation principles as far as the certificates of good conduct are concerned.
- Amend the privacy statement as recommended in this Opinion.

Done at Brussels, 7 September 2007

Peter HUSTINX  
European Data Protection Supervisor