

ADMINISTRATIVE CIRCULAR 02/2007
ON SECURITY CLEARANCE RULES

Having regard to the Rules of Procedure of the European Central Bank¹, and in particular Article 11.2 thereof,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council 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 data²,

the Executive Board has adopted this Administrative Circular.

Article 1

Purpose and objectives

- 1 Under Article 10(b) of the ECB Conditions of Employment, and Article 14(a) of the Conditions of Short-Term Employment, a security clearance is mandatory prior to taking up appointment at the ECB.
- 2 A security clearance shall be mandatory for non-staff members and unescorted visitors to move within the premises of the ECB.
- 3 The purpose of these rules and procedures is to introduce a security clearance procedure in order to enhance the recruitment process and to support the physical security risk management process.

Article 2

General Principles

- 1 The security clearance procedure shall be based on the principles of legality, transparency and professional secrecy.
- 2 The security clearance procedure shall be adequate, relevant and proportionate to the purposes for which the data are collected and/or processed.

¹ Decision of the European Central Bank of 19 February 2004 adopting the Rules of Procedure of the European Central Bank (OJ L 80, 18.3.2004, p.33).

² OJ L 8, 12.1.2001, p.1.

- 3 The security clearance procedure shall respect the fundamental rights and freedoms of natural persons, and shall not entail collecting or storing information concerning the data subject without the data subject's consent.
- 4 The security clearance procedure shall be completed before the date of taking up appointment or entry of the data subject to the ECB's premises. If the certificate of criminal records cannot be submitted before that date, a provisional security clearance valid for a maximum of two months may exceptionally be granted on the basis of the self-declaration, without prejudice to the further proceedings described in this Administrative Circular.
- 5 The security clearance procedure shall require data subjects to respond to the following questions:
 - 5.1 whether or not they have a criminal record;
 - 5.2 whether or not criminal proceedings are pending against them.
- 6 Additionally, the security clearance procedure shall require applicants and selected candidates to respond to the following questions:
 - 6.1 whether or not they have been declared bankrupt; or a petition for bankruptcy has been filed against them; and
 - 6.2 whether or not they are able to fulfil their financial obligations.
- 7 A security clearance shall not be issued if the data subject has been sentenced to imprisonment for a period of one year or longer within 20 years prior to the date of taking up appointment or entry to the ECB.

Article 3

Definitions

For the purposes of this Administrative Circular:

- 1 "Security clearance" means an administrative determination by the ECB that there is no objection, from a security perspective, to a data subject performing the duties or tasks at the ECB for which he/she has been employed or otherwise engaged, or moving unescorted within the premises of the ECB.
- 2 "Selected candidate" means candidates who are selected for employment at the ECB and to whom an offer for employment at the ECB has been made.
- 3 "Non-staff member" means all persons working for the ECB other than on the basis of an employment contract and for whom an ECB security badge has been requested.
- 4 "Unescorted visitor" means any other person for whom a manager has requested an unescorted status at the ECB, and who receives an unescorted visitor badge valid for one day only, except for

permanent members of staff of an NCB that is part of the ESCB and members of an ESCB committee or working group.

- 5 “Security self-declaration” means a form containing questions for the purpose of obtaining a security clearance, to which a person requiring security clearance must respond, and in which he/she declares that all the answers given are true, complete and to the best of his/her knowledge. The form shall be drafted in such a manner as to exclude that data subjects need provide information on criminal convictions that have been expunged from the criminal record in accordance with the applicable national law, minor traffic offences or imprisonment of a preventive nature.
- 6 “Data subject” means the identified or identifiable natural person in relation to whom data are processed in the context of this Administrative Circular.
- 7 “Certificate of criminal record”, hereinafter “the certificate”, means a certificate issued by a national or local competent authority of the state of residence of the data subject that either lists – in accordance with the relevant national or local laws – the criminal offences for which the data subject has been convicted, or that specifies whether or not the issuing authority has objections to the data subject being employed by the ECB.
- 8 “Security clearance file” means a set of related records concerning the security clearance of the data subject.
- 9 “Panel” means a group of four persons comprising staff members of DG Administration, Security Division (A/SET), DG Human Resources, Budget and Organisation, Recruitment and Compensation Division (H/RCO), and DG Legal Services, Legal Advice Division (L/LEA), and the Head of A/SET as chair, which reviews a security clearance file of a selected candidate or staff member. In the event that the data subject is a non-staff member, a panel of three persons comprising staff members of A/SET, the concerned business area, and the Head of A/SET as chair, reviews the security clearance file.

Article 4

Responsibilities

- 1 The Head of A/SET shall be responsible for issuing security clearance and administering the security clearance files, according to the data protection rules set out in this document.
- 2 The Head of H/RCO shall be responsible for ensuring that selected candidates are informed of the ECB’s security clearance rules.
- 3 The English Translation and Editing Section is responsible for translating the certificate into English, if need be. For the purpose of the protection of personal data, the certificate will be made anonymous.

- 4 A manager who requests a security badge for a non-staff member or announces an unescorted visitor shall be responsible for ensuring that they are informed about the security clearance rules.
- 5 The Panel shall review the security clearance file of a selected candidate or staff member in the case of a positive response in the security self-declaration, and/or where an offence or any other adverse information is stated on the certificate. The Panel shall make a recommendation to the Director General Human Resources, Budget and Organisation or, in the case of a managerial or advisory position, to the Executive Board, seeking a decision whether a security clearance is to be issued, the probationary period extended or the employment contract terminated.
- 6 The Panel shall be responsible for reviewing the security clearance file of a non-staff member in the case of a positive response in the security self-declaration, and/or where an offence or any other adverse information is stated on the certificate. The Panel shall make a recommendation to the Director General Administration who shall decide whether a security clearance is to be issued.
- 7 The data subject shall be responsible for providing a security self-declaration to the Head of A/SET and requesting the certificate from his/her competent national authority immediately upon receipt of the letter of appointment, but in no case later than two weeks prior to taking up appointment or entry to the ECB's premises.

Article 5

Security clearance levels

- 1 The following security clearance levels shall apply:
 - 1.1 Level A: requires the data subject to complete a security self-declaration.
 - 1.2 Level B: requires the data subject to complete a security self-declaration and to submit a certificate.
- 2 A security clearance shall only be issued if there is no objection, from a security perspective, to a data subject performing the duties or tasks at the ECB for which he/she has been employed or otherwise engaged, or moving unescorted within the premises of the ECB.
- 3 Data subjects accessing security zone two shall require at least Level A security clearance.
- 4 Data subjects accessing security zones three to five shall require Level B security clearance.

Article 6

Procedure for staff members and selected candidates

- 1 The data subject shall submit the security self-declaration, the signed consent form and the certificate – which shall not be more than two months old on the date it is submitted to the ECB – to the Head of A/SET. Related expenses shall be borne by the data subject. A/SET shall open a security clearance file for the data subject.

- 2 In the case of negative responses in the security self-declaration and where no offences or any other adverse information is stated on the data subject's certificate, the Head of A/SET, or the person(s) to whom authority to do so has been delegated, shall issue a security clearance.
- 3 In the case of a positive response in the security self-declaration and/or where an offence or any other adverse information is stated on the certificate of the data subject and, subject to Article 2(7), the Head of A/SET shall convene the Panel in order to review the file.
- 4 The review of the security clearance file shall take into account the following:
 - 4.1 the position and/or duties offered and/or assigned to the data subject;
 - 4.2 the offences and/or other adverse information stated on the certificate and the corresponding responses made by the data subject on the security self-declaration;
 - 4.3 the risks stemming from a potential recidivism of the offences that are listed; and/or
 - 4.4 the risks stemming from a number of separate minor offences (each of which would be of no relevance if isolated), that provides an indication of the integrity of the data subject.
- 5 The data subject shall be informed that the Panel has been convened and shall have the right to be heard in order to present his/her view on the matter. The data subject's comments shall be retained in the security clearance file.
- 6 The Panel shall forward its recommendation in writing to the Director General Human Resources, Budget and Organisation, or in the case of a managerial or advisory position, to the Executive Board, seeking a decision whether a security clearance is to be issued, the probationary period extended, or the employment contract terminated. This reasoned decision shall be communicated in writing to the Head of A/SET who shall inform the Panel and the data subject of the decision.
- 7 All correspondence shall be stored in the data subject's security clearance file.

Article 7

Procedure for non-staff members and unescorted visitors

- 1 The data subject shall submit the security self-declaration, the signed consent form and, in the event a Level B security clearance is required, the certificate – which shall not be more than two months old on the date it is submitted to the ECB – to the Head of A/SET. Upon receipt of the documents, A/SET shall open a security clearance file for the data subject.
- 2 In the case of negative responses in the security self-declaration and where no offences or any other adverse information is stated on the data subject's certificate, the Head of A/SET, or the person(s) to whom authority to do so has been delegated, shall issue a security clearance.
- 3 In the case of a positive response in the security self-declaration, and/or where an offence or any other adverse information is stated on a non-staff member's certificate, the Head of A/SET shall

convene the Panel in order to review the file in accordance with Article 6(4). The non-staff member shall be informed that the Panel has been convened. The Panel shall forward its recommendation in writing to the Director General Administration, seeking a final decision whether or not to issue a security clearance. This reasoned decision shall be communicated in writing to the Head of A/SET who shall inform the Panel and the data subject of the decision.

- 4 In the case of positive responses in the security self-declaration, and/or where offences or any other adverse information is stated on an unescorted visitor's certificate, A/SET shall review the security clearance file in accordance with Article 6(4). The Head of A/SET shall, together with the requesting manager, decide whether or not to issue a security clearance. In the case of disagreement between the Head of A/SET and the requesting manager, the Head of A/SET shall forward the case to the Director General Administration in order to seek a final decision.

Article 8

Validity of security clearances

- 1 The security clearance for a staff member shall remain valid until termination or expiry of his/her employment contract with the ECB, with a minimum duration of three years. The security clearance shall remain valid if the status of the employment contract changes if there is no lapse of time between expiry of the first contract and commencement of the second.
- 2 The security clearance for a non-staff member and/or an unescorted visitor shall remain valid for three years after which, if necessary, a new security clearance must be applied for in accordance with this document.

Article 9

Security clearance file

- 1 Information collected for the purpose of determining whether or not an individual is to be issued a security clearance shall be stored in a security clearance file. The security clearance file shall be marked "PERSONAL & CONFIDENTIAL", in accordance with the ECB's classification grid.
- 2 The security clearance file will contain all relevant documentation that is required for the purpose of issuing a security clearance and shall not be used for any other means.
- 3 The security clearance file shall be retained by the Head of A/SET, acting as data controller.

Article 10

Secure processing of personal data

- 1 The data controller shall keep the security clearance files in appropriate file safes within the secured area of A/SET.
- 2 The security clearance files shall be accessible only to those staff members of A/SET who are appointed by the data controller. For the purpose of Articles 6 and 7, a security clearance file shall also be accessible to members of the Panel.
- 3 The data subject shall have the right to access his/her security clearance file upon written request to the data controller and request rectification of errors or omissions. Such access shall be given, without constraint, at any time within three months after receipt of the request. In the event of dispute, the right to have recourse to the European Data Protection Supervisor may be exercised at any time.
- 4 The data subject may provide the ECB with updated certificates of criminal record at any time throughout the period of validity of the security clearance. The ECB will include updated certificates in the security clearance file and will keep previous certificates of criminal record only until a decision related to the previous certificate has become final.
- 5 The Head of A/SET may issue further instructions as regards the procedure for the safekeeping of a security clearance file.

Article 11

Transfer of personal data

- 1 Personal data contained in a security clearance file shall only be transferred within the ECB if the data are necessary for the legitimate performance of the tasks of the recipient.
- 2 The personal data collected in the course of the security clearance procedure shall not be transferred to any EU institution or body, EU Member State or third country.

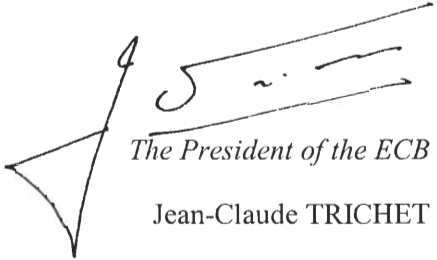
Article 12

Retention and destruction of personal data

- 1 The security clearance file shall be retained 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 with the ECB, but for a minimum of three years. For unescorted visitors, the security clearance file shall be stored for a period of one year after the data subject's last date of access to the ECB.

- 2 After the retention period, the security clearance file shall be destroyed in an appropriate manner under the responsibility of the data controller.

Done at Frankfurt am Main, 19 November 2007.



The President of the ECB
Jean-Claude TRICHET