EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

Introduction to Security Clearance

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 ECB's premises

Objectives of the security clearance rules

The purpose of the security clearance rules and procedures is to enhance the recruitment process and to support the physical security risk management process. 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.

A security clearance shall be mandatory for non-staff members and unescorted visitors to move within the ECB's premises.

General principles of the security clearance rules

The security clearance procedure shall

(a) be based on the principles of legality, transparency and professional secrecy;

(b) be adequate, relevant and proportionate to the purposes for which the data are collected and/or processed;

(c) respect the fundamental rights and freedoms of natural persons, including the right to the protection of their personal data;

(d) 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 record 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 these rules; and

(e) require data subjects to indicate whether:

- **I.** they have a criminal record;
- **II.** criminal proceedings are pending against them;
- **III.** selected candidates have been declared bankrupt or a petition for bankruptcy has been filed against them, unless the probationary period following bankruptcy has been completed successfully; and
- **IV.** selected candidates are able to fulfil their financial obligations.

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.

A security clearance shall not be issued if the data subject has been sentenced to imprisonment for a period of one year or longer for offences which have not been deleted from the certificate of criminal record.

1. Definitions

1) 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;

2) "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;

3) "Unescorted visitor" means any other person for whom a manager has requested unescorted status at the ECB, and who receives an unescorted visitor badge valid for one day only, except for permanent members of staff of a national central bank that is part of the European System of Central Banks and members of an ESCB committee or working group;

4) "Head of DIV/SET" as a position title, includes acting as data controller in the meaning of Regulation (EC) No 45/2001 for the processing of personal data in the context of the security clearance procedure;

5) "Security self-declaration" means a form containing the privacy statement and 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;

6) "Data subject" means the identified or identifiable natural person in relation to whom data are processed in the context of these rules;

7) "Certificate of criminal record" hereinafter called "the certificate", means a certificate of criminal record issued by a national or local competent authority of the country 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 in view of the data subject's criminal record;

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 of DG Administration, Security and Safety Division (DIV/SET), DG Human Resources, Budget and Organisation, Recruitment and Compensation Division (DIV/RCO), and DG Legal Services, Legal Advice Division (DIV/LEA), and the Head of DIV/SET as chair, which reviews a security clearance file of a selected candidate or member of staff. In the event that the data subject is a non-staff member, a panel of three persons comprising DIV/SET staff, the concerned business area, and the Head of DIV/SET as chair, shall review the security clearance file.

2. Responsibilities

1) The Head of DIV/SET shall be responsible for issuing security clearances and administering the security clearance files, according to the data protection rules set out in these rules.

2) The Head of DIV/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 shall be responsible for translating the certificate into English, if need be. For the purpose of the protection of personal data, the certificate shall 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 member of staff with a provisional security clearance 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, and/or where doubt remains regarding the accuracy, authenticity, consistency or comprehensiveness of the submitted documents. 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, and/or where doubt remains regarding the accuracy, authenticity, consistency or comprehensiveness of the submitted documents. 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 the security self-declaration to the Head of DIV/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 entering to the ECB's premises.

3. Security Clearance Levels

1) The following security clearance levels shall apply:

   Level A: requires the data subject to complete a security self-declaration;

   Level B: requires the data subject to complete a security self-declaration and to submit a certificate.

2) Data subjects accessing security zone[1] two shall require at least Level A security clearance.

3) Data subjects accessing security zones three to five shall require Level B security clearance.

4. Procedure for selected candidates

1) The data subject shall submit the security self-declaration 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 DIV/SET. Related expenses shall be borne by the data subject. Upon receipt of any of the documents, DIV/SET shall open a security clearance file for the data subject.

2) Without prejudice to section 3(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 DIV/SET, or the persons to whom authority to do so has been delegated, shall issue a security clearance once they have received originals of all required documents.

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/or where doubt remains regarding the accuracy, authenticity, consistency or comprehensiveness of the submitted documents, the Head of DIV/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:

   a) the position and/or duties offered and/or assigned to the data subject;

   b) 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;

   c) the risks stemming from a potential recidivism of the offences that are listed; and/or

   d) 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 DIV/SET who shall inform the Panel and the data subject of the decision.

All correspondence shall be stored in the data subject's security clearance file**.**

[1] This security concept is based on a six-level security zoning model (SECURITY ZONES 0 - 5), where 0 represents the lowest level of security and 5 the highest. The general purpose is to classify the different areas of the ECB according to their individual risk level. Each zone has a number of different security measures and, as a result, similar areas are clustered.

5. Procedure for non-staff members and unescorted visitors

1) The data subject shall submit the security self-declaration 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 DIV/SET. Upon receipt of any of the documents, DIV/SET shall open a security clearance file for the data subject.

2) Without prejudice to section 3(2), in the case of negative responses in the security selfdeclaration and where no offences or any other adverse information is stated on the data subject's certificate, the Head of DIV/SET, or the persons to whom authority to do so has been delegated, shall issue a security clearance once all required documents are available in original.

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, and/or where doubt remains regarding the accuracy, authenticity, consistency or comprehensiveness of the submitted documents, the Head of DIV/SET shall convene the Panel in order to review the file in accordance with section 4(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 DIV/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, DIV/SET shall review the security clearance file in accordance with section 4(4). The Head of DIV/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 DIV/SET and the requesting manager, the Head of DIV/SET shall forward the case to the Director General Administration for a final decision.

6. Validity of a security clearance

The security clearance for a member of staff shall remain valid until termination or expiry of his/her employment contract with the ECB, but in no case less than three years. A renewed security clearance shall only become necessary, if the preceding security clearance has expired and the new employment contract is not immediately/directly succeeding the preceding one.

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 these rules.

7. 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 shall 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 DIV/SET.

8. Secure processing of personal data

1) The Head of DIV/SET shall keep the security clearance files in appropriate file safes within the secured area of DIV/SET.

2) The security clearance files shall be accessible only to the DIV/SET staff who are appointed by the Head of DIV/SET. For the purpose of sections 4 and 5, 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 Head of DIV/SET 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 at any time throughout the period of validity of the security clearance. The ECB shall include updated certificates in the security clearance file and shall keep previous certificates only until a decision related to the previous certificates has become final.

5) The Head of DIV/SET may issue further instructions regarding the procedure for the safekeeping of security clearance files.

9. 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, body, office or agency, or Member State or third country.

3) The Head of DIV/SET, or the persons to whom authority to do so has been delegated, may contact the relevant authorities to verify the accuracy, authenticity, consistency or comprehensiveness of any document provided by the data subject in order to obtain the security clearance.

10. 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) The Certificate shall be retained for a fixed period of one year after which it will be destroyed, unless there are pending internal procedures (such as an administrative review, grievance or an administrative inquiry procedure) or legal proceedings stemming from a negative decision on granting a security clearance to the data subject. In case of pending internal procedures and legal proceedings, the certificate of criminal records will be destroyed at the latest three months after the administrative decision or judgement is not legally challengeable any longer.