EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

RECORD OF PROCESSING ACTIVITY

EXTENSION OF A PRE-EXISTING ACCESS CONTROL SYSTEM BY AN IRIS SCAN TECHNOLOGY FOR HIGH SECURE BUSINESS AREAS

1. Controller(s) of data processing activities

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity: *Directorate General Corporate Services / Directorate Administration / Security & Safety Division (DG-CS/DA/SET)*

Data Protection Officer (DPO): DPO@ecb.europa.eu

2. Who is actually conducting the processing activity?

☐ The data is processed by the ECB itself

The organisational unit conducting the processing activity is:

☒ The data is processed together with an external third party.

The organisational unit conducting the processing activity is: Directorate General Corporate Services, Security & Safety Division. In addition to internal staff, the maintenance and administration of the system is performed by an external company in a defined and controlled environment.

3. Purpose of the processing

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 encrypted biometric template of the data subject iris is stored in the badge chip of the data subject ECB Security Badge. For further information please refer to the record of processing activity: "Personal data processed via the ECB Security Badge".

For further information please read the *EDPS Prior Checking Opinion*.

4. Description of the categories of data subjects

Whose personal data are being processed?

- ☒ ECB staff
- ☒ Externals (agency staff, consultants, trainees or secondees)
- ☐ NCB or NCA counterparts (in the ESCB or SSM context)
- ☐ Visitors to the ECB, including conference participants and speakers
- ☒ Contractors providing goods or services
- ☐ Complainants, correspondents and enquirers
- ☐ Relatives of the data subject
- ☒ Other (please specify): *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.*

5. Description of the categories of personal data processed

(a) **General personal data:**

The personal data contains:

- ☒ Personal details (name, staff ID, email)
- ☐ Education & Training details
- ☒ Employment details
- ☐ Financial details
- ☐ Family, lifestyle and social circumstances
- ☐ Goods or services provided
- ☒ Other (please give details): *Personal data involved 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.*

(b) **Special categories of personal data**

The personal data reveals:

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☒ Genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health: *Persons with access to highest security zone are authenticated by means of iris recognition system. Encrypted biometric template of the data subject iris is stored in the badge chip.*

For more information, you may read EDPS Opinion on a notification for prior checking related to the extension of a pre-existing access control system by an iris scan technology for high secure business areas

☐ Data regarding a natural person's sex life or sexual orientation

6. The categories of recipients to whom the personal data have been or will be disclosed, including the recipients of the data in Member States, third countries or international organisations

☒ Data subjects themselves

☐ Managers of data subjects

☒ Designated ECB staff members

☐ Designated NCB or NCA staff members in the ESCB or SSM context

☐ Other (please specify):

7. Transfers to/Access from third countries or an international organisation

Data are processed by third country entities:

☐ Yes

Specify to which countries:

Specify under which safeguards:

☐ Adequacy Decision of the European Commission

☐ Standard Contractual Clauses

☐ Binding Corporate Rules

☐ Administrative arrangement containing enforceable and effective data subject rights

If the third country's legislation and/or practices impinge on the effectiveness of appropriate safeguards, the personal data can only be transferred to, accessed from or processed in such third country when sufficient 'supplementary measures' are taken to ensure an essentially equivalent level of protection to that guaranteed within the EEA. These supplementary measures are implemented on a case-by case basis and may be technical (such as encryption), organisational and/or contractual.

☒ No

8. Retention time

Refer to ECB's Filing and Retention Plan

The information is 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 is deleted when re-formatting and/or destroying the badge.