

RECORD OF PROCESSING ACTIVITY

PERSONAL DATA PROCESSED VIA THE ECB SECURITY BADGE

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 and Safety Division / Security Operations Section (DGCS/A/SET/SOP)*

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:
Directorate General Corporate Services/Directorate Administration / Security and Safety Division / Security Operations Section (DGCS/A/SET/SOP)

☐ The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party [mention third party]

Link to privacy statement if available

3. Purpose of the processing

All persons entering the ECB premises are issued with an ECB security badge for access control and security reasons. Information stored in the ECB security badge also entitles the badge holder with access to some ECB Services and Systems.

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):

5. Description of the categories of personal data processed

(a) General personal data:

The personal data contains:

- ☒ Personal details (name, address etc)
- ☐ Education & Training details
- ☐ Employment details
- ☐ Financial details
- ☐ Family, lifestyle and social circumstances
- ☐ Goods or services provided
- ☒ Other (please give details):

Data printed on the security badge:

- Personalized badges:
Name, first name, staff ID and badge ID, picture
- Non-personalized badges:
Badge ID

Additional data electronically stored in the security badge, for the following purposes:

- *Access Control System.*
(please see [Record of processing activity – Administration of access control system](#))
- Authenticated access to the highest security zones via biometric data:
Please refer to the record of processing activity "[Access control system by an iris scan](#)" and to the [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](#)

(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 (*encrypted biometric template of the data subject iris is stored in the badge chip, for data subjects with access to the highest security zone are authenticated by means of iris recognition system*)
- ☒ *Genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health (encrypted biometric template of the data subject iris is stored in the badge chip, for data subjects with access to the highest security zone are authenticated by means of iris recognition system)*
 - ☐ 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](#)

Personal data are kept for the period necessary to fulfil the purposes outlined in part 3.

Personal data is deleted when re-formatting and/or destroying the badge.

The audit trail is kept for 90 days and the visitor personal data is kept in the visitors' DataBase up to 1 year after the visit.