

RECORD OF PROCESSING ACTIVITY

DORA ICT-related incidents and significant cyber threats

1. Controller(s) of data processing activities

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity: DG Horizontal Line Supervision / Operational Resilience & Oversight Division / IT, Operational Risk & Resilience Section

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: DG Horizontal Line Supervision / Operational Resilience & Oversight Division / IT, Operational Risk & Resilience Section
- The data is processed by the National Competent Authorities (NCAs) acting on behalf of the ECB.

3. Purpose of the processing

According to Regulation (EU) 2022/2554 (DORA), financial entities are obliged to report major ICT-related incidents to the relevant competent authority. Financial entities

may, on a voluntary basis, notify significant cyber threats to the relevant competent authority. The relevant reporting templates include personal data of contact points within the financial entity. In addition, names of other persons involved in dealing with the incident may be identified in the free-text fields of the template.

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): Contact points within the bank (mandatory), potentially also other bank employees involved with the incident.

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):

(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
- 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

The overall retention of the system should be 5 years after the end of system/database life, in accordance with series 10.4.0 of the ECB filing and retention plan.