

RECORD OF PROCESSING ACTIVITY

Reporting framework for cyber incidents on Significant Institutions

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

3. Purpose of the processing

After the SB decision obliging significant institutions to report significant cyber incidents has been repealed, incident reports received under this reporting framework are kept in line with the ECB retention policy. Reports include personal data of contact points within the significant institutions. In addition, names of other persons involved in dealing with the incident can be identified within the free text fields of the template.

4. Description of the categories of data subjects

- NCB or NCA counterparts (in the ESCB or SSM context)
- Other: *Contact points within the institution (mandatory), potentially also other bank employees involved with the incident.*

5. Description of categories of personal data processed

- Personal details (name, address etc)
- Employment details

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

- Designated ECB staff members
- Designated NCB or NCA staff members in the ESCB or SSM context

7. Retention time

Cyber incident reports are kept for 20 years from the finalisation of the reports.