

RECORD OF PROCESSING ACTIVITY

Storage and Backup of E(S)CB IT services hosted in ECB Datacentres

1. Controller(s) of data processing activities

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity:

Directorate General Information Systems / Platform Engineering Services Division
(PES)

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 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

Computation, Storage, and Backup of application, business and end-user data in ECB data centre

ECB outsourced the management of IT service delivery in its data centres to an external managed service provider (DXC Technology Deutschland GmbH, HRB 14227, Alfred-Herrhausen-Allee 3-5, 65760 Eschborn, Germany, Account Manager: Thomas Müller - thomas.mueller.external@ecb.europa.eu).

3. Purpose of the processing

Computation of business data in the data centre involves using powerful servers to process and analyse large amounts of digital content, enabling tasks like running business applications, generating reports, and supporting decision-making efficiently and reliably.

Data Storage in the data centre refers to where all the information, like files, documents, databases emails and other digital content, is securely kept and managed. Think of it as a giant, organized library of digital data that businesses and organizations can access and use whenever needed.

Data Backup is a technical protection measure for E(S)CB IT services and data against data loss or damage, with the goal to assure the availability, integrity and completeness of data held within ECB Datacentres. All Personal data collected and stored by business areas as part of E(S)CB IT services is automatically included in the operational storage and backup processing.

DG-IS Platform Engineering Section oversees the IT infrastructure platforms and solutions in the datacentre which are needed to store, protect and manage business data for ECB business areas and end-users. In this function, DG-IS Platform Engineering Section is not considered as owner/controller of the business data including personal data.

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): All of the above as long as it is contained by an E(S)CB IT service hosted and backup in ECB Datacentres.

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): All general and sensitive personal data as long as it is contained by an E(S)CB IT service hosted and backup in ECB Datacentres.

(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
- ☒ DG-IS PES is not the owner / direct controller of the data. All data stored and backed up in the infrastructure are controlled by corresponding business areas and processes. Personal data part of this collection, transferred or disposed as part of the business process storage and backup process of ECB-ESCB IT systems is only accessed by corresponding storage and backup administrators in the cases when operational invention (e.g. data restore) is required. The responsibility for system, storage and backup administration is transferred to an external service provider for IT infrastructure platforms operated in ECB datacentres. In general, in case sensitive data is concerned (e.g. in the systems connected to medical services), further security measures like encryption of primary data from application perspective apply, to provide adequate protection and thus limiting access to data to application and administrative users.

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. Data Retention times

Data is stored and managed in line with business processes defined by owning/collecting business area.

The standards for retention of backup data are defined by the [DG-IS Backup and Restore Policy](#) defined by the Availability Management process. Generally, backups are performed on a daily basis and kept for 35 days for production systems and 15 days for acceptance/test/development systems.

The service level agreement (or operating agreement) for each of the E(S)CB's IT services may specify specific retention periods; for example, that monthly backup copies must be retained for three, six or twelve months.

It should be noted that the retention periods for backup data do not apply to active application data stored on the application host, provided that this data has not been rendered inactive by modification or deletion in the primary storage. The processes for data deletion or cleansing are the responsibility of the business process. The retention period for backup copies only begins once the data on the primary storage platform has become inactive (i.e. has been deleted).