EUROPEAN CENTRAL BANK

EUROSYSTEM

17/07/2023 (DATE OF PUBLICATION/LAST UPDATE)

ECB-PUBLIC

UPDATABLE

RECORD OF PROCESSING ACTIVITY

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 / Infrastructure & Operations Systems

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

Data Backups for applications running in the data centre

ECB outsourced the management of IT service delivery in its data centres to an external managed service provider (Unisys).

Unisys counterpart:

Sheibani, Gholam <Gholam.Sheibani.external@ecb.europa.eu>
(Security Officer EUCSO – Unisys).

3. Purpose of the processing

Backup is a protection measure for E(S)CB IT services and data against data loss or damage, with the goal to improve the availability, accuracy and completeness of data held within ECB Datacentres. Personal data stored as part of E(S)CB IT services is automatically included in the operational backup processing.

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

☒ Other (please specify): Personal data collected, transferred or disposed as part of the backup process of ECB-ESCB IT systems is only accessed by the backup administrators in the cases when an operational restore is required.. The responsibility for system and backup administration is transferred to an external service provider for backups 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 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. Retention time

The standards for retention of backup data are defined by the DG-IS Backup and Restore Policy defined by the Availability Management process. Generally, incremental 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 (or Operational) Level Agreement of each E(S)CB IT service may define specific retentions required, for example monthly backup to be kept for three, six or twelve months.

It should be noted that the expiry rules for backup data do not apply to active application data stored on the application host as long as this data is not made inactive by modification or deletion. The expiry time only starts to run after the data has become inactive.