

11/12/2025

ECB-PUBLIC  
UPDATABLE

## RECORD OF PROCESSING ACTIVITY

### CASPER project

#### 1. Controller(s) of data processing activities

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity: Directorate General Statistics, Statistical Applications & Tools Division

Data Protection Officer (DPO): [DPO@ecb.europa.eu](mailto:DPO@ecb.europa.eu)

#### 2. Who is actually conducting the processing activity?

- The data are processed by the ECB itself: the ECB is the controller for the processing of the personal data. The Directorate General Statistics and the Directorate General Information Systems are responsible for the actual processing.
- The data are processed either by a third party (contractor) or together with an external third party. The data are processed by Amazon Web Services EMEA SARL or by Myra Security GmbH (as sub-processors for the ECB), or by OneWelcome (ECB Identity Portal).

For further information please see:

- <https://aws.amazon.com/privacy/>
- <https://www.onewelcome.com/privacy-policy>
- <https://www.myrasecurity.com/en/gdpr-compliance/>

#### 3. Purpose of the processing

The centralised submission platform (CASPER) allows external organisations and partners to securely submit data to the ECB. Personal data are processed to securely identify and authenticate users. Personal data must be collected when accounts are created through which users can access the platform. The personal data are collected via the Identity and Access Management (IAM, ESCB users) or ECB Identity Portal

(externals) authentication systems. The data are automatically synchronised between the IAM/ECB Identity Portal and CASPER to support the basic functionalities of the system (providing access to different data collections and ensuring traceability of the access to each data collection and reporting entity).

Personal data are also processed for maintenance, performance and security purposes. Some data are needed to ensure our application is technically secure. Myra Security GmbH, a German technology manufacturer providing a security-as-a-service platform, is responsible for processing a limited number of personal data categories (e.g. IP addresses). This processing is crucial for ensuring the technical security of our application. More detailed information on Myra Security GmbH's privacy policy can be found on [Myra Security GmbH's website](#).

#### 4. Description of the categories of data subjects

*Whose personal data are being processed?*

- ECB staff
- Non-ECB staff (agency staff, consultants, cost-free trainees or cost-free secondees working at the ECB)
- NCB or NCA counterparts (in the ESCB or a European banking supervision context)
- Visitors to the ECB
- Contractors providing goods or services
- Complainants, correspondents and enquirers
- Relatives of the data subject
- Other (please specify): reporting agents who submit/monitor data in CASPER

#### 5. Description of the categories of personal data processed

##### (a) General personal data

The personal data contain:

- Personal details (name, address, etc.)
- Education and training details
- Employment details
- Financial details

- Family, lifestyle and social circumstances
- Goods or services provided
- Other (please give details): IP, HTTP headers, cookies, query parameters and payload data, device and network information

**(b) Special categories of personal data (Article 10)**

The personal data reveal:

- 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
- Information regarding an individual's sex life or sexual orientation

**6. Categories of recipient to whom the personal data have been or will be disclosed, including the recipients of the data in EU 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 a European banking supervision context
- Other (please specify): CASPER user administrators from external organisations (i.e. private companies, banks or universities)

**7. Transfers to/access from third countries or an international organisation**

Data are transferred to third country recipients:

Yes

Specify to which countries:

Specify under which safeguards:

Adequacy decision of the European Commission

Standard contractual clauses

Binding corporate rules

Administrative arrangements containing enforceable and effective data subject rights

If a 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" have been taken to ensure that the level of protection is essentially equivalent to that guaranteed within the European Economic Area. 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

In CASPER, personal data (name and email address) will be kept in the CASPER database and audit logs in accordance with the retention period stipulated for the IAM and the ECB Identity Portal and the retention period set separately by the ECB collection owner for each data collection. Once the record has been removed from the IAM/ECB Identity Portal the data will be removed from the user management function in CASPER. The audit logs in CASPER will be deleted, either in accordance with the retention period stipulated by the ECB collection owner for a given dataset or upon request from the data subjects at any time.