

## RECORD OF PROCESSING ACTIVITY

### Processing of personal data in the context of teleworking

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

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity:

Directorate General Human Resources / Employee Services (DG-HR / ESE)

Data Protection Officer (DPO): [DPO@ecb.europa.eu](mailto: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: DG-HR /ESE  
with the technical support of/in coordination with DG-IS

☒ The data is processed by a third party (contractor) or the processing operation is  
conducted together with an external third party: As needed IBM, CapGemini

#### 3. Purpose of the processing

**Compliance with the EU institutions' framework and with the ECB's rules.** The purpose of this processing operation is to manage the rights and obligations of ECB members of staff or trainees relating to the ECB teleworking rules to ensure the continuous functioning of the ECB and the performance of its task and exercise of its mandate as an EU institution.

**ECB's awareness of staff location during their working time for duty of care.** As an employer the ECB has the obligation to know where the ECB personnel [1] works to be able to

contact them when they are not working in the office.

Justification for the collection of entries for teleworking registered by the ECB personnel in ISIS [2] :

- Teleworking entries: in line with legitimate obligation and duty of any employer to know if staff works on the premises or offsite.
- Collection of generic data (Frankfurt area, EU and outside EU): to monitor adherence to the applicable teleworking quotas, related requirements and entitlements.
- Collection of generic data “reason for cancelling a teleworking request”: to identify potential issues with the implementation of the teleworking policy
- Collection of teleworking address when the ECB member of staff or trainee works from an address that is different from the ones specified in the ECB member of staff or trainee’s Personal Profile.

Justification for sharing teleworking country location data outside ISIS: The country location must be provided by the ECB personnel to the manager orally, so that the manager can alert them, if appropriate, to the list of high-risk countries or recall to the ECB premises the staff member best suited and geographically closest in case of business needs.

In the TW dashboard for managers, non-anonymised teleworking data is made available to managers for their own monitoring of compliance with the rules. Individual non-anonymised data can also be accessed by dedicated HR staff in the table view. Access is only granted on a need-to-know basis to individual staff members.

Besides, personal data in the context of teleworking is also collected and processed with the purpose of granting teleworking exceptions which may or may not be related to the health situation of the ECB personnel. HR Experts and Management process the information which is strictly necessary (to assess whether the request for a teleworking exception can be approved).

[1] The wording ‘ECB personnel’ refers to fixed-term and short-term contract employees (including graduate programme participants), and/or trainees.

[2] ISIS is the SAP based system used at the ECB.

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

*Whose personal data are being processed?*

- ☒ ECB staff
- ☒ Non-ECB staff (agency staff, consultants, trainees, cost-free trainees or cost-free secondees working at the ECB)
- ☐ 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): ECB personnel's dependents or close relatives (exceptionally, information about their health situation, in so far as strictly necessary for the assessment of a request for teleworking exception for reasons not related to the health situation of the ECB personnel)

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

**(a) General personal data:**

The personal data contains:

- ☒ Personal details (name, address etc). The generic teleworking location (Frankfurt area, EU and outside EU), the generic reason for cancelling a teleworking request, the telework location country, the address of teleworking if significantly different from the addresses registered in the Personal Profile, data needed to process requests for teleworking exceptions not related to the health situation of a staff member
- ☐ 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 in the context of teleworking exceptions related to the health situation of the ECB personnel or related to the health situation of their dependents/close relatives)
- ☐ 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: all teleworking data they have recorded in the system
- ☒ Managers of data subjects: ISIS teleworking entry data, teleworking country (communicated orally), data needed in the context of teleworking exceptions
- ☒ Less than 10 designated HR/ESE staff members: generic data (in cases of accident, may need to retrieve also address in workflow) and HR management

with regard to data pertaining to teleworking exception requests which may or not be related to the health situation of the ECB personnel

☐ Designated NCB or NCA staff members in the ESCB or SSM context

☒ Other (please specify):

Access to the personal data is restricted to authorised persons with a legitimate **need to know** (e.g. HR processing). To be read also in conjunction **with 3) above**.

## 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 period of data storage is based on the [ECB's Filing and Retention plan](#) (series 3.4.1.1 of the ECB Filing and Retention Plan. Teleworking generic data (registration and generic location for quota purpose, as well as reason for cancelling a teleworking request) are kept for 5 years. The address of teleworking indicated by the ECB staff member is only stored in a workflow which is deleted after 2 years. When the workflow is deleted, the address is deleted. The workflow is deleted after 2 years starting from the approval of the request, which is deemed accepted by management and therefore is effective 2 days after the request for teleworking was made in ISIS. In the context of exceptions to teleworking not related to the health situation of the ECB personnel, personal data is kept 2 years from end of calendar year in a restricted Darwin folder [3]. For exceptions to teleworking related to the health situation of the ECB personnel, the retention period is 5 years from T-end of calendar year, and the data is saved in the personal file.

[3] Darwin is the ECB's IT tool for the management of documents and records.