# Record of processing activity

## Pillar 3 data hub

Record of EBA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 (EUDPR)

| Part 1 - Article 31 Record (publicly available) | | |
|---|---|---|
| 1 | **Last update of this record** | 09/06/2026 |
| 2 | **Date of next review** | 09/06/2028 |
| 3 | **Reference number** | EBA/DPR/2025/5 |
| 4 | **Name and contact details of controller** | Controller: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France<br>Responsible Department: Data Analytics, Reporting and Transparency (DART)<br>Contact: P3DH@eba.europa.eu |
| 5 | **Contact details of DPO** | dpo@eba.europa.eu, or alternatively send a letter to the postal address of the EBA (address above) marked for the attention of the DPO of the EBA. |
| 6 | **Name and contact details of joint controller (where applicable)** | Not applicable |
| 7 | **Name and contact details of processor (where applicable)** | Microsoft EntraID and Governance Tool Software (Identity and Access Management)<br>One Microsoft Place<br>South County Business Park<br>Leopardstown<br>Dublin 18 D18 P521 Ireland<br>Telephone: +353 (1) 706-3117<br>Webform available at https://aka.ms/privacyresponse |
| 8 | **Short description and purpose of the processing activity** | The European Banking Authority (EBA) is mandated in accordance with Articles 434 and 434a of the Capital Requirements Regulation III to publish on its website all the prudential disclosures for all institutions subject to these disclosure requirements, making it |

## Part 1 - Article 31 Record (publicly available)

readily available in a centralized manner to all the relevant stakeholders through a single electronic access point on its website. To comply with this mandate, the EBA is building a data hub putting together all the disclosures required under Part Eight of the CRR.

As the Pillar 3 information will be uploaded directly by large and other institutions in the EUCLID data submission channel, it is necessary to have information on the data submitter(s) from each institution. This information will allow the EBA to have the contact points nominated by institutions. These contact persons will be the ones in charge of submitting the information to the EBA. To ensure that the exchanges between EBA and institutions are agile and efficient, information on more than one contact person would be required (especially for cases of temporary absence of one of these contact persons, this is particularly relevant). In this sense, the indication of a single functional mailbox also required to be provided would not be enough.

The necessary information on data submitters is collected with a template in excel format developed for this purpose and shared with institutions together with the individual onboarding letter sent by the EBA. Information on name (and surname), phone number, email and role in the institution of the person that has access to report the data to the EBA via EUCLID is collected. This data, submitted by institutions via email, should be used to populate the EBA database with contact details of submitters of Pillar 3 information. The above mentioned excel template is focused on contact persons' details and hence, the data is completely identifiable and is subject to data protection measures. Contact persons can also be nominated directly by institutions already onboarded via the Microsoft EntraID and Governance Tool Software.

A second template in XBRL-csv format is used to collect information on the nominated contact persons to receive automatic notifications from the EBA when the Pillar 3 reports for the respective institution are published on EDAP. This template is modelled under the EBA Data Point Model (DPM) and institutions are required to submit it to the P3DH via EUCLID, at least, on an annual basis. These contact persons will also serve as the relevant points of contact should any bilateral communication from the EBA be required.

The institution has full discretion to decide whether the nominated data submitter(s) and the nominated contact person(s) designated to receive EBA automatic notifications are the same individuals or different persons.

| Part 1 - Article 31 Record (publicly available) | | |
|---|---|---|
| 9 | **Description of categories of persons whose data the EBA processes and list of data categories** | This processing activity involves processing of personal data of individuals from people that are the contact points from the reporting institutions such as:<br>➢ Identification data: name and surname<br>➢ Contact data: professional email address, professional telephone<br>➢ Professional data: employer, position |
| 10 | **Special categories of personal data processed (as defined in Article 10 EUDPR)** | No special category of personal data is specifically required for this processing activity. |
| 11 | **Time limit for keeping the data** | The retention period is 1 year or until a new submission of the respective template is received, if this new submission exceeds 1 year from previous submission, in case banks don't report X.01.00 template in a year's time to ensure we keep at least the last user contacts up and running. The EBA shall delete personal data upon expiry of that period. |
| 12 | **Recipients of the data** | The personal data will be processed and stored in the EBA secure IT environment, with restricted access. Data collected will be protected to a level that is appropriate to its sensitivity and will be accessible exclusively to authorised staff. |
| 13 | **Are there any transfers of personal data to third countries or international organisations?** | The personal data will be processed by the EBA within the EU/EEA. |
| 14 | **General description of security measures, where possible** | The personal data will be processed and stored in the EBA secure IT environment, with restricted access. Data collected will be protected to a level that is appropriate to its sensitivity and will be accessible exclusively to authorised staff.<br>The system is designed to be safeguarded against deliberate and intrusive threats from internal and external actors (malicious or otherwise). It can only be accessed using two factor authentication, from user with specific data access permission and using passwords compliant with EBA security policy. Reporting authorities only have access to personal data they have uploaded. EBA's information security policy requires information about financial sector operators, including related personal data, to have appropriate |

| Part 1 - Article 31 Record (publicly available) | | |
|---|---|---|
| | | security marking and to be stored in restricted locations and circulated with encryption. The system keeps an audit of all login attempts. It uses data encryption and IT logs and monitors the activity. |
| 15 | **For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:** | The information is provided to the institutions in specific data protection notices. |