Record of processing activity

External breach reporting (Whistleblowing)

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

Nr	Item	Description
Part 1 - Article 31 Record (publicly available)		
1	Last update of this record	15/09/2023
2	Reference number	EBA/DPR/2023/6
3	Name and contact details of controller	Controller: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France Contact: ExecutiveOffice@eba.europa.eu
4	Name and contact details of DPO	dpo@eba.europa.eu Or by letter to the postal address of the EBA marked for the attention of the DPO of the EBA: The postal address of the EBA is: DEFENSE 4 – EUROPLAZA 20 Avenue André Prothin CS 30154 92927 Paris La Défense CEDEX
5	Name and contact details of joint controller (where applicable)	Not applicable
6	Name and contact details of processor (where applicable)	EQS Group AG Karlstr. 47 80333 München www.eqs.com For more information, please read their privacy statement and their terms and conditions on the following link: https://www.eqs.com/fr/a-propos-deqs/protection-des-donnees/
7	Short description and purpose of the processing	As required by Article 17a of the EBA Regulation, and in accordance with the Whistleblowing Directive where applicable, the EBA has developed its external breach reporting system. This external

Nr	Item	Description
		breach reporting system is to be used by persons who wish to submit information where they, in good faith, have reasonable grounds to believe that there may be a breach of Union law within the EBA's competence to act upon. Personal data is processed to enable the EBA's effective receipt and handling of such reports, and allowing necessary action to be taken upon them. For the purpose of this activity there is a dedicated reporting channels for receiving and handling such information. This reporting channel protects persons submitting reports from any potential retaliation through all information being able to be submitted anonymously or confidentially, and safely. In line with its powers and tasks pursuant to the EBA Regulation the EBA may act on reports, by: • Making inquiries to verify the allegations made and that the report falls within the EBA's competences to act upon; • By taking action under Article 9b of the Regulation regarding potential breaches of certain Union anti-money laundering and counter-terrorist financing law; • Exercising its powers regarding alleged breaches of Union law by competent authorities under Article 17 of the EBA Regulation; • Carrying out inquiries into certain potential financial stability threats under Article 22 of the EBA Regulation.
8	Description of categories of persons whose data the EBA processes and list of data categories	**Categories of data subjects** • EBA staff and contractors. • Counterparts of EBA staff in competent authorities. • Reporting persons: The natural persons submitting reports or doing so on behalf of legal persons. • Persons concerned: Persons referred to in reports as persons to whom breaches are attributed to or persons associated with such persons. • Persons involved: Other persons named in reports and who are involved in or may be affected by EBA procedures. • Other persons: Others who may appear in reports or in the EBA files on such reports, but who are not material to the case concerned. **Data categories/fields** The following data may be processed (if and when applicable): • Personal details (name, address, date of birth, nationality, etc) • Employment details • Financial details

Nr	Item	Description
		• Allegations and/or material indicative of potential breaches of administrative or criminal law The EBA provides an online form for reporting persons to complete their reports. This includes free text fields that may be filled in with other categories of personal data.
9	Time limit for keeping the data	Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay. After a case file has been closed, all relevant personal data will be stored for the following retention periods. If a report received is considered relevant to the EBA's regulatory tasks, the data will be stored for five years. This is an appropriate period for the fulfilment of the EBA's short, medium and long-term tasks and multi-year work programmes which are based on the EBA's legal mandates. - If a report is considered relevant to other EBA tasks, the data will be stored for a shorter period of twelve months in order to support such tasks in line with the EBA's legal mandates. - If the EBA decides that a report is not relevant to any of its tasks, the data will be stored for three months in view of any potential follow-up action which the EBA may be required to take, e.g. the handling of related legal claims.
10	Recipients of the data	The following persons may have access to the personal data: • Designated EBA staff. • Designated non-EBA staff, including members of the EBA governance bodies and staff/members of competent authorities within the meaning of Article 4(2) of the EBA Regulation.
11	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
12	General description of security measures, where possible	In order to protect personal data, the EBA has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

Nr	Item	Description
		For instance, only EBA staff designated by the Head of the Legal and Compliance Unit on a need-to-know basis have access to personal data stored on the online platform provided and operated by EQS Group AG on behalf of the EBA. Multi-factor authentication will be required for EBA users to access the EQS system. The same applies also to information, which is stored outside the EQS system, including information stored in hardcopy. EBA authorised staff will be subject to the legal obligation of professional secrecy with regard to all confidential information in their possession or knowledge. In addition, EQS are ISO2001 certified, which demonstrates they have in place strong information security controls. All processing operations are carried out pursuant to the EBA Decision (EBA/DC/138) of 29 October 2015 on the security of communication and information systems in the EBA. The EBA adopted Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
13	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	The data protection notice is available on the EBA website. EBA - Privacy policy (integrityline.com)
Part 2 - compliance check, risk screening and documentation (internal)		
Compliance check (Articles 4 and 5)		
14	Legal basis and necessity for processing	☒ (a) necessary for performance of tasks in the public interest attributed by EU or MS legislation ☐ (a2) necessary for the management and functioning of the EBA for the performance of tasks in (a) ☐ (b) necessary for compliance with legal obligation incumbent on controller ☐ (c) necessary for performance of a contract to which the DS is party ☐ (d) consent ☐ (e) vital interest Processing of personal is necessary for performance of tasks in the public interest attributed by Union legislation by virtue of: Article 17a of Regulation (EU) No 1093/2010 (the EBA Regulation); Article 9b of the EBA Regulation regarding indications of breaches of certain Union anti-money laundering and counter-terrorist financing law;

Nr	Item	Description
		Article 17 of the EBA Regulation regarding alleged breaches of Union law by competent authorities; Article 22 of the EBA Regulation regarding inquiries into certain potential financial stability threats; Directive (EU) 2019/1937 of the European Parliament and of the Council (the Whistleblowing Directive)
15	Purpose definition	Personal data is not processed for purposes other than those mentioned in point 7.
16	Data minimisation	The categories of personal data that may be processed relate to the content of allegations arising from reports, related contacts with competent authorities, persons concerned, information on the means for verifying allegations and so forth. In line with Article 17 of the Whistleblowing Directive personal data which is manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.
17	Accuracy	Personal data of reporting persons are, in the first instance, collected directly from those data subjects. Personal data of persons of interest and other persons as provided in reports are subject to verification through further EBA inquiry where the report becomes subject to further action. Where the report is instead closed, the personal data is not used for other purposes and is deleted. The EBA's approach provides safeguards as to accuracy. The EBA will advise reporting persons to ensure accuracy of personal data in the first instance. Inaccurate reports will be rectified without undue delay, with copies of inaccurate reports being deleted. Secondly, where EBA considers that a report does warrant further inquiry, such inquiry will seek to establish the accuracy of the material facts, including the accuracy of personal data. Thirdly for reports not warranting further inquiry, the personal data will be deleted within three months of closing the file, save where personal data is considered relevant to the EBA's regulatory tasks or other tasks as explained below. The consequences of inaccuracy for persons of interest could be high as the reporting person or other sources of information may indicate that the persons of interest have acted in breach of regulatory or legal requirements, administrative or criminal law.
18	Storage limitation	Personal data which is manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay. After a case file has been closed, all relevant personal data will be stored for a set retention period. If a report received is considered relevant to the EBA's regulatory tasks, the data will be stored for five years. This is an appropriate period for the fulfilment of the

Nr	Item	Description
		EBA's short, medium and long-term tasks and multi-year work programmes which are based on the EBA's legal mandates. If a report is considered relevant to other EBA tasks, the data will be stored for a shorter period of twelve months in order to support such tasks in line with the EBA's legal mandates. If the EBA decides that a report is not relevant to any of its tasks, the data will be stored for three months in view of any potential follow-up action which the EBA may be required to take, e.g.the handling of related legal claims.
19	Transparency: How do you inform people about the processing?	EBA staff and reporting persons will be informed in advance: A privacy notice is made available on the EBA's Internet and on the EQS system where reporters may input data. Moreover, a privacy notice is available on the EBA website. Other data subjects that may be mentioned in a report may not be communicated to. Transparency is restricted in this manner where communicating to these data subject would jeopardise the investigation and subsequently the purpose of the processing. This is allowed under Article 25.1 (EUDPR) and EBA Restrictions Decision (EBA/DC/2021/377).
20	Access and other rights of persons whose data you process	Data subjects may exercise their rights by contacting the DPO either via e-mail at dpo@eba.europa.eu or via mail by sending a letter to the postal address of the EBA marked for the attention of the DPO of the EBA. The postal address of the EBA is: DEFENSE 4 – EUROPLAZA 20 Avenue André Prothin CS 30154 92927 Paris La Défense CEDEX If the exercise of data subjects' rights would jeopardise the purpose of the processing, the exercise of such rights may be delayed in line with the EBA Restrictions Decision See Privacy Statement available on the EBA website.
High risk identification		
21	Does this process involve any of the following?	☐ data relating to health ☐ data relating to sex life or sexual orientation, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☒ criminal convictions, (suspected) criminal offences or otherwise considered sensitive ('special data categories') ☐ evaluation, automated decision making or profiling ☐ monitoring data subjects

Nr	Item	Description
		☐ new technologies that may be considered intrusive. The EBA's breach reporting system is not principally designed for handling reports of criminal cases. The EBA provides an online form which reporting persons are to use in order to make a report, and this does not specifically target any of the above-listed data. The EBA must however ensure that the system allows reporting persons to provide information to support their claim that they, in good faith, have reasonable grounds for believing that a breach of relevant Union law may have been committed. It is inherent to this that reporting persons may adduce information liable to support an allegation that a person has committed a criminal offence, or historical information as to criminal convictions/actual commission of criminal offences. The processing of the special categories of data is justified on the basis of Article 10(2)(g): Processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued.
Linked documentation		
22	(where applicable) links to threshold assessment and DPIA	The Threshold assessment is saved in the folder of the processing activity on the U drive: U:\EBLG\Unit\0340 - Data Protection\1. Processing activities
23	Where are your information security measures documented?	EBA/DC/138 and Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission See further item 12.
24	Other linked documentation	EBA Whistleblowing Policy: link ESQ Privacy Policy https://www.eqs.com/fr/a-propos-deqs/protection-des-donnees/ ESQ General terms and conditions https://www.eqs.com/about-eqs/terms-and-conditions/ EBA Restrictions Decision (EBA/DC/2021/377): link