Record of processing activity

Security inquiries

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	11/08/2023
2	Reference number	EBA/DPR/2023/8
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 Responsible Department: Operations Contact: IT.Support@eba.europa.eu
4	Name and contact details of DPO	dpo@eba.europa.eu
5	Name and contact details of joint controller (where applicable)	Not applicable
6	Name and contact details of processor (where applicable)	Not applicable
7	Short description and purpose of the processing	The purpose of the processing is to investigate potential security breaches and/or to identify potential unauthorised disclosure of confidential information. The processing activities related to the security inquiries pertain to the collection, storage, and analysis of personal data necessary for the investigation. The scope of each security inquiry will be limited according to the specific mandate adopted. The information gathered may be used in administrative investigations, disciplinary proceedings and/or OLAF proceedings. The processing activities relate to the security inquiries pertain to the

Nr	Item	Description
		collection, storage, and analysis of personal data necessary for the investigation. The following legal bases apply with respect to the security inquiry: Article 53(3) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC; and Decision EBA DC 138 adopting the Commission Information Security Policy, in particular Article 7 of Commission Decision C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.
8	Description of categories of persons whose data the EBA processes and list of data categories	Categories of data subjects: All staff members potentially involved in events under investigation (including the person being investigated, witnesses, and alleged victims) and any other persons quoted in the file. Categories of personal data include: Identification Data: This includes information such as surname, first name, gender, age, name of line manager, hiring date, contractual category and grade, organisational entity; contact details (phone numbers, email addresses), staff number. Authentication Data: Data related to login credentials and other authentication information that may be used to verify the identity of data subjects involved in the security inquiry. Device Information: Details about the devices used by individuals, such as IP addresses, device IDs, and browser information. Access Logs: Records of data subject's access to EBA databases. System Logs: Records of system activities, events, and errors that may assist in identifying anomalies, unauthorized access, or potential security breaches. Email and Communication Data: Content and metadata of emails, instant messages, and other communication channels that may be relevant to the security inquiry. Work and Mobile Phone Data: Calls list from communication providers. Witness Statements: Statements or testimonies provided by witnesses or individuals involved in the incident. Internet access data: Browsing history. Other Relevant Data: Any other data that is directly or indirectly related to the security inquiry and deemed necessary for its investigation and resolution.

Nr	Item	Description
9	Time limit for keeping the data	The EBA will keep the personal data for a maximum of 12 months following submission of security inquiry report, subject to administrative investigations, disciplinary proceedings and/or OLAF proceedings.
10	Recipients of the data	The investigation is conducted by mandated investigators. The personal data may be also accessible to a restricted group of IT experts. The report of the investigation and the data gathered in the security inquiry may be shared within the EBA to the extent needed to follow up on the conclusions of the security inquiry. Under certain circumstances the report, the statements collected and the evidence found may be forwarded for follow-up to a competent body, where the data is relevant to a separate investigation or inquiry. In particular to investigators appointed to carry out an administrative inquiry, EPPO, OLAF, the psychosocial service of the Medical Service. In cases where the EBA files a complaint or acts as a civil party, the data in the file may be communicated to the national judicial authority and/or the police. When a person, working inside the EBA for an external contractor is involved in a hearing, that person may be accompanied by someone representing that external contractor. This representative will be a recipient of the content of the hearing.
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	Processing is performed under the EBA Information Security Framework, published on the EBA intranet. The computer system and servers are safeguarded and can only be accessed by the mandated investigators, along with a restricted group of IT experts. All paper files are stored in locked cabinets, in an office accessible only to the security officers responsible for handling them. Entry to the premisses is protected by a badge reader, and its usage is recorded.
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 general data protection notice is available on the intranet on the following path: Staff Matters / Conditions of Employment / Regulations and Policies