10 October 2025

GENERAL DATA PROTECTION STATEMENT RELATED TO DORA OVERSIGHT

Introduction

1. The European Supervisory Authorities (the European Banking Authority (EBA), the European Insurance and Occupational Pension authority (EIOPA) and the European Securities and Market Authority (ESMA), collectively "the ESAs"), are committed to protecting individuals' personal data in accordance with Regulation (EU) 2018/1725[1] (further referred as "the Regulation").

2. In line with Articles 15 and 16 of the Regulation, this data protection statement provides information to the data subjects relating to the processing of their personal data carried out by the ESAs.

Purpose of the processing of personal data

3. The personal data is processed as part of their DORA Oversight Activities to ensure robust supervision and oversight of critical ICT third-party providers (CTPPs) and other relevant entities in the EU financial sector. This processing supports the designation, risk assessment, planning, and execution of oversight examinations, as well as the follow-up of recommendations. The goal is to ensure that these providers meet the requirements for digital operational resilience.

4. Additionally, personal data processing facilitates effective coordination and cooperation among the ESAs, national competent authorities, independent experts, and third-country authorities. This collaboration is essential for protecting the financial sector against ICT disruptions, cyber threats, and operational risks, thereby safeguarding consumers, investors, and the overall stability of the EU financial system.

5. Through these activities, is aim to:
    - Achieve a harmonized and high level of digital operational resilience across the EU financial sector.
    - Ensure compliance with DORA requirements for incident reporting, resilience testing, and ICT risk management.

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

Legal basis of the processing of personal data and/or contractual or other obligation imposing it

6. Legal basis for the processing: The processing of personal data in the context of DORA Oversight Activities is carried out in accordance with Article 5(1)(a) EUDPR. The processing is necessary for the performance of tasks carried out in the public interest and in the exercise of official authority vested in the ESAs under the Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554, specifically Articles 31 to 44.

Controller of the personal data processing

7. Each ESA is an independent controller for processing activities where it defines the means and purposes alone. Each is responsible for EUDPR compliance, handling breaches, and data subject requests for those activities.

8. For activities where the ESAs jointly define the means and purposes, they are joint controllers.

9. The joint controllership covers activities such as managing the DORA Oversight Forum, the Joint Oversight Network, Joint Examination Teams and their collaboration spaces, digital tools for tracking oversight actions, data rooms for information exchange, interactions with critical third-party providers, coordination with third-country authorities, and finance management related to oversight. For these joint activities, any ESA can receive and handle data subject requests. The ESA that receives a request will address it, with support from the others as needed, unless collectively decided otherwise. All ESAs cooperate to ensure requests are managed efficiently and in line with the EUDPR.

10. Address and email address of the controllers:

Joint Controller	Joint Controller	Joint Controller
EBA DEFENSE 4 – EUROPLAZA 20 Avenue André Prothin, CS 30154 92927 Paris La Défense CEDEX France info@eba.europa.eu	**EIOPA** Westhafen Tower, Westhafenplatz 1 60327 Frankfurt am Main Germany fausto.parente@eiopa.europa.eu	**ESMA** 201-203 Rue de Bercy, 75012 Paris, France DP.ED@esma.europa.eu

Contact details of the Data Protection Officer (DPO)

EBA	ESMA	EIOPA
Tour Europlaza, 20 avenue André Prothin, 92400 Courbevoie, France dpo@eba.europa.eu	201-203 Rue de Bercy, 75012 Paris, France dpo@esma.europa.eu	Westhafen Tower, Westhafenplatz 1 60327 Frankfurt am Main Germany dpo@eiopa.europa.eu

Types of personal data collected

11. Categories of Persons Whose Data Is Processed

Category	Who is Included
Oversight Bodies	- Oversight Forum (OF) members, alternates, observers - Joint Oversight Network (JON) members - Joint Examination Team (JET) members
Independent Experts (IE)	- Individuals nominated or contracted as independent experts
Third-Party Providers (TPPs/CTPPs)	- Contact points and handlers at TPPs/CTPPs - Employees of CTPPs involved in oversight activities
Competent Authorities (CAs)	- Staff nominated to participate in oversight activities (e.g., JETs) - Staff of EU and non-EU CAs with access to Data Room Solutions
Third-Country Authorities (TCAs)	- Contact points supporting or participating in inspections or coordination
Other Individuals	- Individuals mentioned in documentation provided by CTPPs (e.g., board/executive meeting minutes, operational documentation) - Users of collaboration platforms (JET Collaboration Space, Data Room, Tracker/ticketing tool)

12. List of Data Categories that could be processed in different processing activities

Type	Examples
Identification Data	- Name, position, email, address, telephone number

Additional Data	- CV, application letter, Bank account details, Conflict of interest forms, Info on assignments/tasks, Performance information, ID numbers, Onboarding information for fee collection, Personal data uploaded by users, Personal data included in documentation provided by CTPPs.
Technical Data	- File/folder ownership information, Comment author information, @tagging of usernames, logs information, User access data (username, password, 2FA tool, IP address).

Recipients/processors of the personal data collected

13. Personal data may be shared with the European Supervisory Authorities (EBA, EIOPA, ESMA), competent national authorities, designated critical third-party providers, formally appointed experts, relevant third-country authorities, and contracted IT service providers, only for DORA Oversight purposes.

14. Processors and sub-processors processing personal data:

    - Microsoft - provision of Azure and M365 services
    - Brainloop AG – Provider of Brainloop Data Room Services
    - Telekom Deutschland GmbH – Hosting provider; data center services.
    - For certain parts of the processing the EBA processes personal data on behalf of ESMA and EIOPA.

Retention period

15. Personal data processed in the context of DORA Oversight activities will be retained for a period of up to 10 years. After the 10-year retention period, personal data will be securely deleted or, where appropriate, transferred to the EU Archives in accordance with applicable archiving rules. If legal proceedings or investigations require, data may be retained for a longer period until the conclusion of such matters.

Transfer of personal data to a third country or international organisations

16. Personal data will be processed within the EU/EEA or in countries with adequacy decisions. Transfers to third-country authorities or international organisations may occur when necessary for DORA oversight activities, such as coordination with non-EU supervisory authorities or

participation in joint inspections. Such transfers are carried out on the basis of appropriate agreements and safeguards.

Automated decision-making

17. No automated decision-making including profiling is performed in the context of this processing operation.

What are the rights of the data subject?

18. You have the right to access your personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate. You also have the right to request the erasure of your personal data, as well as object to or obtain the restriction of their processing. These rights are subject to certain limitations.

19. For the protection of the data subjects' personal data protection rights, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.

20. Restrictions of certain rights of the data subject may apply, in accordance with Article 25 of the EUDPR.

21. Should you wish to exercise any of the rights provided in the paragraphs above, please contact EBA's DPO (dpo@eba.europa.eu) or EIOPA's DPO (dpo@eiopa.europa.eu) or ESMA's DPO (dpo@esma.europa.eu).

Who to contact in case of questions or complaints regarding data protection?

22. Any questions or complaints concerning the processing of your personal data can be addressed to any of the ESA Data Controller or DPO using the contact details indicated above.

23. Data subjects can have recourse to the European Data Protection Supervisor **(**www.edps.europa.eu**)** at any time, as provided in Article 63 of the Regulation**.**