DORA Oversight

Record of activities processing personal data, based on Article 31 of 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.

Nr.	Item	Record Information
DORA Oversight		
1	**Last update of the record**	09/11/2025
2	**Reference number**	ESMA40-1159621584-2015
3	**Name and contact details of controller**	Controller: European Securities and Markets Authority (ESMA), 201-203 Rue de Bercy, 75012 Paris, France Contact: DP.ED@esma.europa.eu Joint controllership with: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France

		The European Insurance and Occupational Pensions Authority (EIOPA) Westhafenplatz 1, 60327 Frankfurt am Main, Germany
4	**Area entrusted with processing**	DORA Joint Oversight Department *Joint ESAs Department, reports to the three ESAs Executive Directors
5	**Processors (if any)**	Microsoft - provision of Azure and M365 services
6	**Name and contact details of DPO**	Data Protection Officer of ESMA: dpo@esma.europa.eu Data Protection Officer of the EBA: dpo@eba.europa.eu Data Protection Officer of EIOPA: dpo@eiopa.europa.eu
7	**Name and contact details of processor (where applicable)**	Microsoft One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Ireland Telephone: +353 (1) 706-3117

		https://aka.ms/privacyresponse Link to Privacy Documentation For certain parts of the processing the EBA processes personal data on behalf of ESMA and EIOPA. European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France https://www.eba.europa.eu/homepage
8	**Purpose of the processing**	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. 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. These activities aim to: 1. Achieve a harmonized and high level of digital operational resilience across the EU financial sector. 2. Ensure compliance with DORA requirements for incident reporting, resilience testing, and ICT risk management. 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

<table>
<tr><td></td><td></td><td>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.

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.

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

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.</td></tr>
<tr><td>9</td><td>Description of categories of persons processed and list of data categories</td><td>Categories of Persons Whose Data Is Processed

<table><tr><th>Category</th><th>Who is Included</th></tr><tr><td>Oversight Bodies</td><td>- Oversight Forum (OF) members, alternates, observers
- Joint Oversight Network (JON) members
- Joint Examination Team (JET) members</td></tr></table></td></tr>
</table>

		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)

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).
10	**Time limit for keeping the data**	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.	
11	**Recipients of the data**	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.	
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	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.	

13	**General description of security measures, where possible.**	Personal data is protected by a range of technical and organisational measures, including role-based access controls, multi-factor authentication, encryption of data in transit and at rest, regular access reviews, audit logging, and secure IT infrastructure. All processing is carried out in accordance with EU information security policies and the internal security frameworks of the ESAs.
14	**Information on how to exercise your rights to access, rectification, object and data portability (where applicable), including recourse right.**	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice available on the website: Joint General Privacy statement - DORA Oversight Specific data protection notices may be provided directly to the data subjects.