AMLA
Anti-Money Laundering Authority

RECORD OF PROCESSING ACTIVITIES
OPERATION OF INTERNAL COMMITTEES

1. PROCESSING PARTIES

1.1 CONTROLLER NAME	RESPONSIBLE UNIT
Authority for Anti-Money Laundering Authority and Countering the Financing of Terrorism (AMLA) MesseTurm Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Germany	Policy on Private Sector Standards Unit Policy on Supervision Unit
1.2 DATA PROTECTION OFFICER name	**CONTACT DETAILS**
DPO	dpo@amla.europa.eu
1.3 PROCESSOR NAME (IF APPLICABLE)	**CONTACT DETAILS**
CISCO Webex (in the case of organisation of online meetings with the Webex tool)	https://privacyrequest.cisco.com
1.4 JOINT CONTROLLERS NAME (IF APPLICABLE)	**CONTACT DETAILS**
Not applicable	Not applicable

2. PROCESSING ACTIVITY

2.1 **NAME OF THE ACTIVITY**

Operation of AMLA's internal committees reporting to the General Board in the supervisory composition: the Internal Committee on Private Sector Standards (ICPSS) and the Internal Committee on the Functioning of the Supervisory System (ICSUP)

2.2 **PURPOSE OF THE PROCESSING OF PERSONAL DATA**

The purpose of this processing activity is to organise the work of two internal committees (ICPSS and ICSUP) supporting the work of the AMLA General Board in supervisory composition, and in particular:

(a) holding of physical and online meetings of the committees and the committee substructures (working groups, task forces)

(b) collecting nominations to the committee substructures

(c) conduct of the written procedures

(c) granting access to documents for members of committees or committee substructure through dedicated document management systems.

2.3 **OTHER PURPOSES**

For the collection of data on dietary preferences.

2.4 LEGAL BASIS

Choose applicable as per Article 5(1) of Reg. (EU) 2018/1725:	*Check (YES/NO)*	
Art. 5(1)(a) For the performance of a task carried out in public interest or under AMLA Regulation	YES	*Please name the task:* Article 58(1) of the Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism
Art. 5(1)(b) For complying with a legal obligation upon the Unit/Authority	NO	*Please specify:* Not applicable
Art. 5(1)(c) For contractual reasons of the Data Subject	NO	*Please specify:* Not applicable
Art. 5(1)(d) The Data Subject has given consent for one (or more) purposes as listed above	YES	*Please explain how the consent is gathered:* For the collection of data on dietary preferences. Consent will be requested as part of the survey collecting the data.
Art. 5(1)(e) For protecting the vital interests of the data subject	NO	*Please specify:* Not applicable

2.5 **NECESSITY OF THE PROCESSING OF PERSONAL DATA**

AMLA has the responsibility to protect the public interest by ensuring supervisory convergence and high-quality supervision in the area of anti-money laundering and countering the financing of terrorism across the internal market (Article 1(3) of the Regulation (EU) 2024/1620 of 31 May 2024). To fulfill this responsibility, AMLA's General Board may establish internal committees to deliberate specific issues and reach conclusions that are reported to the General Board for a final decision (Article 58(2) of the Regulation (EU) 2024/1620). Processing of basic personal data of the committee members is necessary to organise their work in the form of meetings and written procedures, as well as for establishing committee substructures (working groups, task forces).

2.6 **DATA SUBJECTS**

Members nominated by the Member States to ICPSS/ ICSUP and committee substructures

Observers nominated by the EU institutions/ bodies and EEA Member States to ICPSS/ ICSUP and committee substructures

AMLA staff and Seconded National Experts participating in the work of ICPSS/ ICSUP and committee substructures

2.7 **CATEGORIES OF PERSONAL DATA**

For all data subjects:

Name

Surname

Dietary preferences in the context of catering for physical meetings

In addition, for Members and Observers:
- represented national institution or EU institution/ body
- work email address

2.8 DATA RETENTION

Data category	*Time limit*
Name, surname, represented national institution or EU institution/ body, work email address	Will be retained for time of the operation of the ICPSS and ICSUP
Dietary preferences.	Will be retained for 10 days after the meeting

3. DISCLOSURE OF PERSONAL DATA - RECIPIENTS WHERE PERSONAL DATA IS DISCLOSED

3.1 INTERNAL UNITS

(Please list all internal entities to whom the data will be disclosed):

Policy on Private Sector Standards Unit

Policy on Supervision Unit

3.2 MEMBER STATES AUTHORITIES OR THIRD PARTIES (i.e.: private sector) WITHIN THE EU

Administrators of the AMLA's building in relation to granting the access for physical meetings (MesseTurm Service GmbH, Friedrich-Ebert-Anlage 49, Frankfurt am Main).

European Insurance and Occupational Pensions Authority/ EIOPA (Westhafenplatz 1, Frankfurt am Main) in relation to granting the access for physical meetings (for as long as EIOPA's premises are used for AMLA meetings).

Occasionally, other administrators of the meeting venues.

3.3 THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

(If this is the case, please document the additional safeguards in compliance with Art. 48 of the DPR):

Cisco Webex stores the following personal data in the United States of America (USA), in the case of organisation of online meetings with the Webex tool:

(a) analytics platform data, utilising host and usage information

(b) billing information

The additional safeguard relies on the US Privacy Framework, in which Cisco is registered: https://www.cisco.com/c/en/us/about/trust-center/gdpr.html

4. PRIVACY STATEMENT/ DATA PROTECTION NOTICE

FOR MORE INFORMATION INCLUDING HOW TO EXERCISE YOUR RIGHTS TO ACCESS, RECTIFICATION, OBJECT AND DATA PORTABILITY (WHERE APPLICABLE).

FOR DRAFTING OF THE PRIVACY STATEMENT, PLEASE FOLLOW ART. 15-16 OF THE DPR.

4.1 **Please insert a link if available, or the text of the Privacy Statement:**

Purposes of data processing

(1) Organisation of committee meetings

Your personal data, included name, surname, represented national institution or EU institution/ body and work email address, are processed by AMLA (Policy on Private Sector Standards Unit and Policy on Supervision Unit), that is the Controller, for the purpose of organisation of the work of two internal committees supporting the AMLA' General Board in the supervisory composition: (i) the Internal Committee on Private Sector Standards (ICPSS) and (ii) the Internal Committee on the Functioning of the Supervisory System (ICSUP).

Specific activities supported through personal data collection include:

(a) holding of physical and online meetings of the two committees and committee substructures (working groups, task forces)

(b) collecting nominations to the committee substructures

(c) conduct of the written procedures

(d) granting access to documents for members of committees or committee substructure through dedicated document management systems.

The recipients of your data will be the AMLA's units: Policy on Private Sector Standards Unit (for ICPSS) and the Policy on Supervision Unit (for ICSUP).

AMLA will retain for time of the operation of the ICPSS and ICSUP the data related to your identification: name, surname, institutional affiliation and work email address.

(2) Access to meeting venues

Administrators of meeting venues will be processing your data on our behalf. This includes:

(a) administrators of the AMLA's building (MesseTurm Service GmbH, Friedrich-Ebert-Anlage 49, Frankfurt am Main)

(b) the European Insurance and Occupational Pensions Authority/ EIOPA (Westhafenplatz 1, Frankfurt am Main) for as long as EIOPA's premises are used for AMLA meetings

(c) occasionally, other administrators of the meeting venues.

(3) Use of the Webex tool

Cisco Webex stores the following personal data in the United States of America (USA), in the case of organisation of online meetings with the Webex tool:

(a) analytics platform data, utilising host and usage information

(b) billing information

The additional safeguard relies on the US Privacy Framework under EU, in which Cisco is registered:
https://www.cisco.com/c/en/us/about/trust-center/gdpr.html

With an exception of data transfers related to the use of the Webex tool as described above, your data will not be transferred to third countries or

international organisations and will not be used for an automated decision-making, including profiling.

(4) Data on dietary preferences in the context of meeting catering

In addition, AMLA may collect data on your dietary preferences in connection with the organisation of the meeting catering. The consent for the collection of such data will be requested, when relevant, thorough a non-mandatory survey. AMLA will retain such data for 10 days following the meeting date.

Contact to Controller

You can contact the Controller at:

(a) IC-Private-Sector-Standards@amla.europa.eu (for ICPSS)

(b) supervisory.policy@amla.europa.eu (for ICSUP)

Your rights

You have the right to access, rectify, erase, and restrict your data, as well as to the right to object to the processing and the right to data portability subject to the conditions set in Articles 17 to 24 of the 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.

If you would like to exercise any of these rights, contact the controller or the DPO at dpo@amla.europa.eu.

You have the right to lodge a complaint with the European Data Protection Supervisor (https://edps.europa.eu) if you consider that your personal data protection rights have been infringed.

4.2 **Please explain how you intend to provide the Privacy Statement to the Data Subjects (i.e. via email, teams, Website, etc.):**

The privacy statement will be made available to the data subjects by way of distribution through the data management system and a dedicated agenda point in a specific committee meeting.

5. DATA SECURITY

5.1 **ORGANISATIONAL MEASURES**

Access to data is restricted to authorised staff within the relevant teams on a need-to-know basis.

Staff with access to personal data for outreach activities are made aware of their data protection obligations and handle personal data in accordance with the data protection rules defined for this activity.

5.2 TECHNICAL MEASURES

	Check (YES/NO)	*Description (if YES)*
Pseudonymisation or Encryption	NO	
Measures to ensure:		
– Confidentiality of Data	YES	Access to data is restricted to authorised personnel through access controls and user authentication.
– Integrity of Data	YES	Access information kept in a single database.
– Availability of Data	YES	Data is stored on reliable platforms with appropriate backup and recovery procedures in place.
Resilience of Systems and Services	YES	The platforms used benefit from the resilience measures of the hosting environment.
Restoration of availability and access to Personal Data in a timely manner	YES	Backup and recovery procedures of the platform provider ensure timely restoration in the case of incident.
Process for testing, assessing and evaluation of the effectiveness the measures	NO	