

# RECORD OF PROCESSING ACTIVITIES

## REPORTING REQUIREMENTS UNDER ARTS. 7, 45, 62 AMLD6

### 1. PROCESSING PARTIES

#### 1.1 CONTROLLER NAME

Authority for Anti-Money Laundering Authority and  
Countering the Financing of Terrorism (AMLA)  
MesseTurm  
Friedrich-Ebert-Anlage 49  
60308 Frankfurt am Main  
Germany

#### RESPONSIBLE UNIT

Indirect Supervision Team; contact: [Indirect-Supervision@amla.europa.eu](mailto:Indirect-Supervision@amla.europa.eu)

#### 1.2 DATA PROTECTION OFFICER name

AMLA DPO

#### CONTACT DETAILS

[dpo@amla.europa.eu](mailto:dpo@amla.europa.eu)

#### 1.3 PROCESSOR NAME (IF APPLICABLE)

EU COM – EU Survey  
EU COM also acts as Controller for EU Login, the  
authentication tool to use EU Survey  
CISCO Webex

#### CONTACT DETAILS

For EU Survey (EU COM)  
<https://ec.europa.eu/eusurvey/home/support>  
EU COM DPO [DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:DATA-PROTECTION-OFFICER@ec.europa.eu)  
<https://privacyrequest.cisco.com/>

#### 1.4 JOINT CONTROLLERS NAME (IF APPLICABLE)

Click or tap here to enter text.

#### CONTACT DETAILS

Click or tap here to enter text.

### 2. PROCESSING ACTIVITY

#### 2.1 NAME OF THE ACTIVITY

Reporting requirements under Articles. 7, 45, 72 AMLD5

#### 2.2 PURPOSE OF THE PROCESSING OF PERSONAL DATA

The purpose of the processing of personal data is to

- a) identify the contact person of the AMLA member who is responsible for the response of the respective authority to the AMLA survey is to ensure that AMLA can raise questions or comments with the competent natural persons in the responding authority directly.
- b) identify the natural person that has been subject to a sanction or an administrative measure in order to implement the reporting requirement for sanctions and administrative measures taken on the national level as set forth in Art. 62 AMLD5, to make sure that the sanction or measure reported in case of individuals can be differentiated from the sanctions and measures applied to other individuals, and to use this information in the course of AMLA`s direct supervision of obliged entities when deciding on the fitness and properness of members of the management, of Compliance and AML-officers.

#### 2.3 OTHER PURPOSES

#### 2.4 LEGAL BASIS

Choose applicable as per Article 5(1) of Reg. (EU) 2018/1725:

 Check  
(YES/NO)

<b>Art. 5(1)(a)</b> For the performance of a task carried out in public interest or under AMLA Regulation	<input checked="" type="checkbox"/> / <input type="checkbox"/>	Please name the task: <a href="#">Article 40(2) AML Directive</a>
<b>Art. 5(1)(b)</b> For complying with a legal obligation upon the Unit/Authority	<input type="checkbox"/> / <input checked="" type="checkbox"/>	Please specify the legal obligation: <a href="#">Click or tap here to enter text.</a>
<b>Art. 5(1)(c)</b> For contractual reasons of the Data Subject	<input type="checkbox"/> / <input checked="" type="checkbox"/>	<a href="#">Click or tap here to enter text.</a>
<b>Art. 5(1)(d)</b> The Data Subject has given consent for one (or more) purposes as listed above	<input type="checkbox"/> / <input checked="" type="checkbox"/>	Please explain how the consent is gathered: <a href="#">Privacy statement on AMLA website</a>
<b>Art. 5(1)(e)</b> For protecting the vital interests of the data subject	<input type="checkbox"/> / <input checked="" type="checkbox"/>	Please specify: <a href="#">Click or tap here to enter text.</a>

## 2.5 NECESSITY OF THE PROCESSING OF PERSONAL DATA

By legal obligation, AMLA must collect reporting of EU-Member States. The person making the report and acting as a contact person needs to be identified for questions and other necessary communication. Regarding sanctions and administrative measures personal data (name and surname) is a necessary part of the information on sanctions or administrative measures applied to an individual. It is accordingly a necessary component of the reporting obligation.

## 2.6 DATA SUBJECTS

- Staff (TA/CA)
- SNEs
- Trainees
- Outsourced personnel

- Member States/ Competent authorities contacts  
[Selected contact persons of the AMLA-members](#)
- Other contacts (please specify)
- Other (please specify)

**Persons reported by NCAs about whom they have imposed a sanction or administrative measure**

## 2.7 CATEGORIES OF PERSONAL DATA

- Name
- Surname
- Place/Date of Birth
- Gender
- Country of Work (not necessarily nationality)
- ID Card/Passport Number/ Personal Number
- Picture

- Communication Data (Email Account, Telephone Number, Address Work or Personal - please specify) [Email, IP address/Device ID, duration of the browsing session](#)
- Title, Function (please specify)
- Financial information (Bank Account or Others – please specify)
- Bio
- CV
- Location
- Others [Sanctions and measures applied to respective individual](#)

## 2.8 DATA RETENTION

Data category

Time limit

All data categories	5 Years
---------------------	---------

### 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):*

Indirect Supervision Unit, Risk Analysis Unit, Direct Supervision Unit.

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

1. Only in case the information could give rise to criminal proceedings: FIUs and National judicial authorities.
2. In accordance with the need to know principle: AMLA can pass on data to national AML/CFT supervisory authorities.

#### 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):

- o Cisco Webex analytics platform data, which utilises host and usage information;
- o 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>

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

None

### 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:

[Available on the Survey page](#)

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

The surveys will be sent out to member state competent authorities with a reference and link to the privacy statement on the AMLA website.

### 5. DATA SECURITY

#### 5.1 ORGANISATIONAL MEASURES

EU Survey stores the EU Login username as well as e-mail addresses of the survey owners at the Data Centre of the European Commission.

The European Commission has implemented security measures to protect server hardware, software and the network from accidental or malicious manipulations and loss of data. All data is stored on European Commission servers managed by DG DIGIT in line with the technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January

2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, its implementing rules and the corresponding security notices. These documents (as adapted from time to time) are available for consultation at the following address: [https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems\\_en](https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en) . Additionally, the personal data will be stored internally in the AMLA IT environment once extracted.

## 5.2 TECHNICAL MEASURES

	<i>Check (YES/NO)</i>	<i>Description (if YES)</i>
Pseudonymisation or Encryption	<input checked="" type="checkbox"/> /□	
Measures to ensure:		
– Confidentiality of Data	<input checked="" type="checkbox"/> /□	
– Integrity of Data	<input checked="" type="checkbox"/> /□	
– Availability of Data	<input checked="" type="checkbox"/> /□	
Resilience of Systems and Services	<input checked="" type="checkbox"/> /□	
Restoration of availability and access to Personal Data in a timely manner	<input checked="" type="checkbox"/> /□	
Process for testing, assessing and evaluation of the effectiveness the measures	<input type="checkbox"/> /☒	