

## RECORD OF PROCESSING ACTIVITIES

# TASK FORCE ON NON-FINANCIAL SECTOR RISK ASSESSMENT METHODOLOGY

### 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

NFS Risk Assessment Team; contact: [riskmodels-nfs@amla.europa.eu](mailto:riskmodels-nfs@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

Task Force on non-financial sector Risk Assessment methodology

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

The purpose of the processing of personal data is to enable the registration and participation of representatives of competent authorities to regular meetings in relation to risk assessment methodology for the non-financial sector and to manage the participation in the meeting. The proper participation requires registration of the data subjects to be able to participate in the meeting and establishes list of attendants necessary information to plan the event both online and in Frankfurt.

#### 2.3 OTHER PURPOSES

Share contact details between members of the task force to facilitate internal exchange and to offer hospitality.

#### 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"/>	<i>Please name the task:</i> <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"/>	<i>Please specify the legal obligation:</i> <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 checked="" type="checkbox"/> / <input type="checkbox"/>	<i>Please explain how the consent is gathered:</i> <a href="#">In relation to hospitality and to facilitating cooperation among the participants, data subjects are also asked to provide information regarding their dietary preferences and to be able to share the contacts among the participants' group. Consent is requested at the time of registration for the meeting, distinguishing between both aspects, and with the provision of a privacy statement on the registration page.</a>
<b>Art. 5(1)(e)</b> For protecting the vital interests of the data subject	<input type="checkbox"/> / <input checked="" type="checkbox"/>	<i>Please specify:</i> <a href="#">Click or tap here to enter text.</a>

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

By legal obligation, AMLA must draft regulatory technical standards setting out benchmarks and methodology for assessing and classifying inherent and residual risk profile of obliged entities, as well as the frequency at which such risk profile shall be reviewed. In order to draft the RTS, it is necessary for AMLA to discuss and collaborate with representatives of the Member States to ensure that the final RTS meets the needs and obligations mandated by law. Properly meeting with counterparts allows for a more balanced outcome and input on the task placed upon AMLA>

**2.6 DATA SUBJECTS**

- |   |   |
|---|---|
| <input type="checkbox"/> Staff (TA/CA)<br><input type="checkbox"/> SNEs<br><input type="checkbox"/> Trainees<br><input type="checkbox"/> Outsourced personnel | <input checked="" type="checkbox"/> Member States/ Competent authorities contacts<br><a href="#">Selected members of the AMLA Task Force “Non-Financial Sector Risk Assessment”.</a><br><input type="checkbox"/> Other contacts (please specify)<br><input type="checkbox"/> Other (please specify) |
|---|---|

**2.7 CATEGORIES OF PERSONAL DATA**

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Name<br><input checked="" type="checkbox"/> Surname<br><input type="checkbox"/> Place/Date of Birth<br><input type="checkbox"/> Gender<br><input checked="" type="checkbox"/> Country of Work (not necessarily nationality)<br><input type="checkbox"/> ID Card/Passport Number/ Personal Number<br><input type="checkbox"/> Picture | <input checked="" type="checkbox"/> Communication Data (Email Account, Telephone Number, Address Work or Personal - please specify) <a href="#">Email, IP address/Device ID, duration of the browsing session</a><br><input checked="" type="checkbox"/> Title, Function (please specify) <a href="#">Institution; Sector of expertise (i.e.: auditing, gambling, real estate, etc.).</a><br><input type="checkbox"/> Financial information (Bank Account or Others – please specify)<br><input type="checkbox"/> Bio<br><input type="checkbox"/> CV<br><input type="checkbox"/> Location |
|--|---|

Others Dietary preferences for catering (vegetarian, vegan, others to be specified by the data subject). Preference for sharing contact details.

**2.8 DATA RETENTION**

Data category	Time limit
All data categories	Duration of the existence of the Task Force

**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):*

AMLA Risk Assessment Team.

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

If the individual provides additional explicit consent, we will additionally share contact details with other members of the task force. The details to share include: Name, email address, country organization based at, and sector of expertise.

**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 registration will be organized via a survey link using the online tool "EU Surveys". The respondents will need to tick a box that they agree to the privacy statement, which will be provided via link as a downloadable pdf-document. Additionally, they will explicitly need to tick a box to allow us to share their contact details with other members of the task force.

## 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"/> /☒	