

RECORD OF PROCESSING ACTIVITIES

AGM

1. PROCESSING PARTIES

CONTROLLER NAME AMLA (Anti-Money Laundering Authority) Address: MesseTurm Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Germany	RESPONSIBLE UNIT Executive Director
DATA PROTECTION OFFICER name DPO	CONTACT DETAILS DPO@amla.europa.eu
PROCESSOR NAME (IF APPLICABLE) PMO – Paymaster’s Office	CONTACT DETAILS PMO-DATA-PROTECTION-COORDINATOR@ec.europa.eu
JOINT CONTROLLERS NAME (IF APPLICABLE) N/A	CONTACT DETAILS N/A

2. PROCESSING ACTIVITY

2.1 NAME OF THE ACTIVITY
 Advanced Gateway Meetings (AGM) – reimbursement and administrative management of internal and external meetings

2.2 PURPOSE OF THE PROCESSING OF PERSONAL DATA
 The purpose of the processing of personal data is the conduct of the administrative procedures necessary to arrange:

- arrangement of medical checks of candidates of selection procedures which require reimbursement after their appointment is finished.
- arrangement of in-person interviews with candidates of selection procedures which reimbursement after their interviews have completed.

2.3 OTHER PURPOSES
 N/A

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

☐/ ☐

Please name the task:
[Click or tap here to enter text.](#)

Art. 5(1)(b) For complying with a legal obligation upon the Unit/Authority	☒ / ☐	<i>Please specify the legal obligation:</i> Articles 86, 147 and 148 of the Financial Regulation
Art. 5(1)(c) For contractual reasons of the Data Subject	☒ / ☐	Article 33 of the Staff Regulation for the medical check Annex III of the Staff Regulations Implementing rules related to the engagement and use of Temporary agents, contracts agents and middle management staff
Art. 5(1)(d) The Data Subject has given consent for one (or more) purposes as listed above	☒ / ☐	<i>Please explain how the consent is gathered:</i> For attendance of medical appointments For attendance of in-person interviews
Art. 5(1)(e) For protecting the vital interests of the data subject	☐ / ☐	<i>Please specify:</i> Click or tap here to enter text.

2.5 NECESSITY OF THE PROCESSING OF PERSONAL DATA

AMLA needs to collect the data that is indispensable in order to process and control the reimbursement of activities that are linked to invitation for a medical check prior recruitment. As there is a financial component for the reimbursement, in order to check its validity, some personal data of the data subject are required for identification, other personal data is required for the traceability that the appointment took place, and some other data is required to calculate the proper reimbursement in accordance with the Financial Regulation rules. The software used is PMO property, who is responsible for the execution of the payments, whereas AMLA acts as the entry door to the data subject, for the arrangement of the appointment for a medical check.

For Reimbursements to the candidates: this part of the application is only used by PMO to process expenses claims introduced by the candidates following a medical check organised by AMLA. But some data of the meeting is consulted by PMO's Back Office to check what type of expenses can be reimbursed.

2.6 DATA SUBJECTS

☐ Staff (TA/CA) ☐ SNEs ☐ Trainees ☐ Outsourced personnel	☐ Member States/ Competent authorities contacts ☐ Other contacts (please specify) Click or tap here to enter text. ☒ Other (please specify): Candidates who have been provided with the job offer and need to undertake the Medical check; Candidates who have been invited to participate in in-person interviews
---	--

2.7 CATEGORIES OF PERSONAL DATA

☒ Name ☒ Surname ☒ Place/Date of Birth ☐ Gender ☒ Nationality ☒ ID Card/Passport Number/ Personal Number ☒ Picture	☒ Title, Function (please specify) Job Title ☒ Financial information (Bank Account or Others – please specify) Name, IBAN, Bank name, SWIFT, account holders' name, supporting documents in the absence of a bank stamp (i.e.: copy of recent bank statement confirming account name, IBAN and bank name). ☒ Location ☒ Others (Cover letter, professional certificates, language certificates, motivation letters and the data categories that may be inserted in those documents)
---	--

☒ Communication Data (Email Account, Telephone Number, Address Work or Personal - please specify) [Personal email address](#)

[Country of residence](#)
[Country and city of origin \(of birth\)](#)
 Business data: self-employment, registration number, registration document, VAT (not mandatory)
 Travel data: Place and country of departure, place and country of work, departure/arrival time, ticket/hotel price and supporting documents (hotel invoice, train/plane ticket, private car).
 Place of recruitment

2.8 DATA RETENTION

Data category

Time limit

[All data categories](#)

[7y as per Financial Regulation](#)

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):

[Human Resources Unit for selection procedures](#), [Finance unit for reimbursement](#).

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

[PMO \(Pay Masters Office\)](#)

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):

[N/A](#)

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:

[Privacy statement provided with the invitation to the medical check](#)
[Privacy statement provided with the invitation to the in-person interview](#)

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

[See above](#)

5. DATA SECURITY

5.1 ORGANISATIONAL MEASURES

User profiles defined for different roles with access based on the need-to-know principle
 User's access based on EU Login

5.2 TECHNICAL MEASURES

	Check (YES/NO)	Description (if YES)
Pseudonymisation or Encryption	☐ /	Click or tap here to enter text.
Measures to ensure:		
– Confidentiality of Data	☐ /	Click or tap here to enter text.
– Integrity of Data	☐ /	Click or tap here to enter text.
– Availability of Data	☐ /	Click or tap here to enter text.
Resilience of Systems and Services	☐ /	Click or tap here to enter text.
Restoration of availability and access to Personal Data in a timely manner	☐ /	Click or tap here to enter text.
Process for testing, assessing and evaluation of the effectiveness the measures	☐ /	Click or tap here to enter text.