EUPOL COPPS Privacy Statement

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO PROCUREMENT PROCEDURES BY THE EU MISSION FOR THE SUPPORT OF PALESTINIAN POLICE AND RULE OF LAW (EUPOL COPPS)

1. INTRODUCTION

THE PROTECTION OF YOUR PRIVACY INCLUDING YOUR PERSONAL DATA IS OF GREAT IMPORTANCE TO THE EUROPEAN UNION AND TO CSDP MISSIONS. WHEN PROCESSING PERSONAL DATA WE REFLECT THE PROVISIONS OF THE CHARTER ON FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, AND IN PARTICULAR ITS ART. 8. THIS PRIVACY STATEMENT DESCRIBES HOW THE CSDP MISSION PROCESSES YOUR PERSONAL DATA FOR THE PURPOSE IT HAS BEEN COLLECTED AND WHAT RIGHTS YOU HAVE AS A DATA SUBJECT. YOUR PERSONAL DATA ARE PROCESSED IN ACCORDANCE WITH THE PRINCIPLES AND PROVISIONS LAID DOWN IN THE PERTINENT LEGISLATION ON DATA PROTECTION, INCLUDING THE REGULATION (EC) 45/2001 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA BY THE COMMUNITY INSTITUTIONS AND BODIES AND ON THE FREE MOVEMENT OF SUCH DATA AND ITS SUCCESSIVE LEGISLATIVE ACT. ALL DATA OF A PERSONAL NATURE - NAMELY DATA THAT CAN IDENTIFY YOU DIRECTLY OR INDIRECTLY - WILL BE HANDLED FAIRLY AND LAWFULLY WITH THE NECESSARY CARE.

2. PURPOSE OF THE PROCESSING OPERATION

The purpose of the present processing operation is to ensure that the tenders submitted through the public procedure are in accordance to the same set of criteria provided therein in order to ensure the optimal use of EU financial resources.

3. DATA PROCESSED

The data, including personal data, which may be processed for that purpose are the following:

- Name (first name, family name, previous family name(s));
- Nationality, gender, date of birth, gender, civil status, educations, passport/ID number, country of birth;
- Title, professional function;
- Contact information (e-mail, telephone number(s), fax number, postal address, internet address;
- Bank account reference (IBAN, BIC, VAT number);
- Other relevant data contained in the CV (experience, technical skills, languages, present and past employment);
- Data related to offences and criminal convictions in form of an extract of judiciary record;
- Medical data.

Appropriate organisational and technical security measures will be ensured according to the data protection legislation applicable to EU institutions and bodies.

Outline of Security Measures

Electronic Files: The collected personal data are stored on the servers that abide by the pertinent security rules. Personal data will be processed by assigned staff members. Files will have authorised access. Measures are provided to prevent non-responsible entities from accessing data. General access to all collected personal data and all related information is only possible to the recipients with a UserID/Password.

Physical Files: When not in use, physical copies of the collected personal data will be stored in a properly secured and locked storage container.

Technical and organisational measures are also guaranteed and the appropriate provisions on security of the successor regulation on data protection for EU institutions and bodies in order:

- to prevent any unauthorised person from gaining access to computer systems; any unauthorised reading, copying, alteration or removal of storage media; any unauthorised memory inputs; any unauthorised disclosure, alteration or erasure of stored personal data; unauthorised persons from using data-processing systems by means of data transmission facilities;
- to ensure that authorised users of a data-processing system can access no personal data other than those to which their access right refers; the possibility to check logs; and that personal data being processed on behalf of third parties can be processed only on instruction of the controller; furthermore that, during communication or transport of personal data, the data cannot be read, copied or erased without authorisation;
- to record which personal data have been communicated, at what times and to whom.

4. CONTROLLER OF THE PROCESSING OPERATION

The Controller determining the purpose and the means of the processing operation is EUPOL COPPS. Mission's Procurement Unit is responsible for managing the personal data processing operation which is under the supervision of the *Acting Head of Mission Katja Dominik*.

5. RECIPIENTS OF THE DATA

Recipients of the personal data during the procurement process are:

- Mission staff working in the Procurement Unit or directly involved in the procurement procedure.
- Mission staff working in the Finance Unit on matters related to the paymnets or other transactions.
- Mission's verification officer.
- Mission's Authorizing Officers.
- Mission's Archiving Assistant.
- External auditors from various EU bodies or as appointed by EU Commission.

The given information will not be communicated to third parties, except where necessary for the purposes outlined above. Personal data is not intended to be transferred to a Third Country.

6. PROVISION, ACCESS AND RECTIFICATION OF THE DATA

You have the right to access your personal data and the right to correct any inaccurate or incomplete personal data, as well as to request the removal of your personal data, if collected unlawfully, which will be implemented within 10 working days after your request will have been deemed legitimate. If you have any queries concerning the processing of your personal data, you may address them to the functional mailbox: data-protection@eupolcopps.eu

7. LEGAL BASIS FOR THE PROCESSING OPERATION

Legal basis:

- Regulation (EU. Euratom) 2018/1046 of the European Parliament and of the Council of 19 July 2018 on the Financial Rules Applicable to the General Budget of the Union.
- European Commission Procurement Rules for Common Foreign and Security Policy (CSFP) Operations (v.3.0) of 10 April 2019.
- European Commission Service for Foreign Policy Instruments Vademecum on Financial and Accounting procedures for CSDP Missions (ver. 1.0, 19 March 2018).
- Procurement and Grants for European Union external actions - A Practical Guide (ver. 2020.0 - 1 August 2020).
- Council Joint Action 2005/797/CFSP of 14 November 2005 on the European Union Police Mission for the Palestinian Territories as amended by Council Decision 2013/354/CFSP and subsequent amendments.
- EUPOL COPPS' OPLAN.
- SOP on Procurement.
- Civilian Operations Commander Instruction 12/2018 on the SOP on Personal Data Processing.
- SOP on Personal Data Protection (SOP/02).

8. TIME LIMIT FOR STORING DATA

Retention period of files of successful tendered including their personal data is assured for 7 years after the signature of the respective contract.

Retention period of files of unsuccessful tenderers is 5 years after the end of the particular procedure to allow for all possible appeals.

In case of court litigation, the retention period of files of both successful and unsuccessful tenderers is 5 years after the accomplishment of all judicial procedures.

9. DATA PROTECTION CONTACT: MISSION DATA PROTECTION ADVISOR

In case you have questions related to the protection of your personal data, you can also contact the Mission Data Protection Advisor (MDPA) at the functional mailbox of the mission data-protection@eupolcopps.eu

10. RECOURSE

You have at any time the right of recourse that you may send to the Head of the Mission within EUPOL COPPS, with the MDPA (Legal Advisor) in copy.