

# EUPOL COPPS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF  
PROCESSING DISCIPLINARY DATA  
OF THE EU MISSION FOR THE SUPPORT OF PALESTINIAN POLICE AND RULE OF LAW (EUPOL COPPS)' MEMBERS  
COLLECTED AND MAINTAINED BY THE CPCC DIRECTORATE OF THE EUROPEAN EXTERNAL ACTION SERVICE  
(EEAS) AND BY EUPOL COPPS

## 1. INTRODUCTION

THE PROTECTION OF YOUR PRIVACY INCLUDING YOUR PERSONAL DATA IS OF GREAT IMPORTANCE TO THE EUROPEAN EXTERNAL ACTION SERVICE (EEAS) AND TO EUPOL COPPS. WHEN PROCESSING PERSONAL DATA WE RESPECT THE PRINCIPLES OF THE CHARTER ON FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, AND IN PARTICULAR ARTICLE 8 ON DATA PROTECTION.

THIS PRIVACY STATEMENT DESCRIBES HOW THE EEAS AND EUPOL COPPS PROCESS YOUR PERSONAL DATA FOR THE PURPOSE IT IS COLLECTED AND WHAT RIGHTS YOU HAVE AS A DATA SUBJECT. YOUR PERSONAL DATA, INCLUDING DISCIPLINARY INFORMATION, IS PROCESSED IN ACCORDANCE WITH 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, AND REPEALING REGULATION (EC) NO 45/2001 AND DECISION NO 1247/2002/EC AS OF 11 DECEMBER 2018, ALIGNED WITH PROVISIONS OF THE GENERAL DATA PROTECTION REGULATION /REG. (EU) 2016/679/ BY THE EEAS AND IN ACCORDANCE WITH THE CIVOPSCDR INSTRUCTION 12-2018 AND ITS SUBSEQUENT AMENDMENT(S) ON THE SOP ON THE PROTECTION OF PERSONAL DATA FOR CSDP MISSIONS BY THE CIVILIAN CSDP MISSIONS.

ALL DATA OF PERSONAL NATURE - DATA THAT CAN IDENTIFY YOU DIRECTLY OR INDIRECTLY - IS HANDLED WITH THE NECESSARY CARE.

## 2. PURPOSE OF DATA PROCESSING: Why do we process your data?

### PURPOSE

The main purpose of processing your personal data is to implement the "Code of Conduct and disciplinary procedure for EU civilian CSDP Missions" (hereafter referred to as the Code of Conduct). For the sake of clarity, the personal data in the context of the implementation of the Code of Conduct is referred to as "disciplinary data".

The Code of Conduct aims at guaranteeing a healthy and safe work environment in all civilian CSDP Missions where all mission members can reasonably expect from their peers, high personal standards of ethical behaviour, impartiality and integrity, as well as acting in an irreproachable manner during and outside working hours.

### DESCRIPTION

The Civilian Operation Commander is responsible to ensure that duty of care of the EU is properly discharged. The EUPOL COPPS Head of Mission (HoM) is responsible for disciplinary control over the staff of EUPOL COPPS. The Civilian Operation Commander and the HoM shall guarantee the safe and secure work environment to the mission personnel (taking into account the volatile environment where EUPOL COPPS is deployed).

On 16 December 2024, the Council of the European Union approved the revised "Code of Conduct and Disciplinary procedure for EU civilian CSDP Missions" that includes measures to guarantee the impartiality and objectivity of investigations conducted by the Missions and by the Conduct and Integrity Entity established by the Code of Conduct. Applying this Code of Conduct involves by essence to process disciplinary data. Its article 45 foresees: "*In the framework of this Code, personal data shall be collected only to the extent necessary and relevant and in accordance with the principles and procedures of personal data protection as contained, in particular, in the Civilian Operation Commander Instruction 12-2018 for the Missions and in Regulation (EU) 1725/2018 for what concerns the EEAS*".

Personal data are processed when a Mission member or a third party submits a report, during the preliminary assessment of facts and the disciplinary investigation, including appeals and the decisions of the respective Responsible Authority. Personal data may be collected for the purpose of providing evidence in documents, statements, observations, on-site inspections and interviews, both in electronic (emails, photo, screenshots etc) and physical file. The report of the breach and any further information collected during the preliminary assessment and/or the investigation is kept in the case file. The case files are kept by the Responsible Authority.

The processing activity aims at rendering effective Article 45 of the Code of Conduct by complying with all requirements foreseen by the rules on personal data protection.

### 3. DATA PROCESSED: What data do we process?

#### Administrative data:

- Identification data (such as name and surname, date and location of birth, nationality, category of staff, position within the Mission, occupation for third parties concerned)
- Contact data (such as phone number, residence address, professional e-mail address, private email address)
- Any other personal data necessary for the case file.

#### Case file related data:

- All personal data processed by the Conduct and Integrity Entity when completing its tasks foreseen by the Code of Conduct (Article 5bis of the Code of Conduct)
- All personal data included in the report (Article 6 of the Code of Conduct)
- All personal data collected during the preliminary assessment of facts (Articles 12 to 15 of the Code of Conduct)
- All personal data collected during the disciplinary investigation (Articles 16 to 20 of the Code of Conduct)
- All personal data submitted to the Disciplinary Board and included in its written advice (Articles 29 to 31 of the Code of Conduct)
- All personal data included in the decision of the Responsible Authority in first instance (Article 32 to 34 of the Code of Conduct)
- All personal data included in the written appeal introduced by the mission member under disciplinary procedure (Article 35 of the Code of Conduct)
- All personal data submitted to the Disciplinary Board of Appeal and/or included in its written advice (Articles 39 and 40 of the Code of Conduct)
- All personal data included in the decision taken by the Responsible Authority in second instance (Article 40 of the Code of Conduct)
- All personal data included in supporting document(s), such as correspondence with Member States on decisions taken by the Responsible Authority
- Any other personal data emerging from the implementation of the Code of Conduct.

#### Specific data:

Specific data refer to the data used to identify and to contact Mission members appointed to a specific role in the framework of the Code of Conduct (Responsible Authority, assessors, investigators, members of the Disciplinary Board, members of the Disciplinary Board of appeal):

- Name and surname
- Role in the framework of the Code of Conduct
- Contact data (e-mail address and phone number)

The aforementioned data may be processed for the following data subjects:

- Staff members of EUPOL COPPS under a disciplinary procedure:
  - HoM
  - Staff members seconded by Member States or Contributing third states
  - Staff members seconded by European Union Institutions or the EEAS
  - International contracted staff members
  - Locally contracted staff members
- Mission members, staff of the EEAS or staff appointed by a Member State in the roster, appointed to a specific role in the framework of the Code of conduct:
  - Responsible Authority
  - Assessor
  - Investigator
  - Member of the Disciplinary Board
- Any other person involved or related to the fact(s) / event(s) / behaviour(s) having led to the implementation of the Code of Conduct. Examples: suspect, victim of the breach, witness, interviewee, provider of information or evidence.

### 4. DATA CONTROLLER: Who is entrusted with processing your data?

The Controller determining the purpose and the means of the processing activity is the European External Action Service. Responsibility for the implementation lies with EUPOL COPPS.

The representative of the controller, the EEAS Directorate responsible for managing the personal data processing under the supervision of the Director is the following entity:

**EEAS Civilian Planning and Conduct Capability Managing Directorate (CPCC.MD)  
and the Conduct and Integrity Entity.**

EUPOL COPPS is responsible, for processing in the context of specific disciplinary procedures, the personal and disciplinary data necessary for the implementation of the Code of Conduct within EUPOL COPPS.

## **5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?**

The recipients of the data, on strict need to know basis, are:

### **EEAS**

- Staff of the EEAS Conduct and Integrity Entity (MD.CPCC), given the tasks assigned to this Entity (Article 5bis of the Code of Conduct)
- Experts from the roster referred to in Article 5bis and Annex I of the Code of Conduct (EEAS experts, experts appointed by Member States and experts made available by Missions) appointed as preliminary assessors (Article 12 of the Code of Conduct) by the Responsible Authority
- Experts from the roster referred to in Article 5bis and Annex I of the Code of Conduct (EEAS experts, experts appointed by Member States and experts made available by Missions) appointed as disciplinary investigators (Article 16 of the Code of Conduct) by the Responsible Authority
- Experts from the roster referred to in Article 5bis and Annex I of the Code of Conduct (EEAS experts, experts appointed by Member States and experts made available by Missions) appointed as members of the Disciplinary Board either as chairperson, as voting member or as non-voting secretary (Article 29 of the Code of Conduct)
- Experts from the roster referred to in Article 5bis and Annex I of the Code of Conduct (EEAS experts, experts appointed by Member States and experts made available by Missions) as members of the Disciplinary Board of Appeal either as chairperson, as voting member or as non-voting secretary (Article 39 of the Code of Conduct)

### **CPCC**

- The Civilian Operation Commander, in all cases foreseen by the Code of Conduct
- The Deputy Civilian Operation Commander, in all cases foreseen by the Code of Conduct
- Assigned Advisors of MD.CPCC – only on a need to know/need to do basis, in their capacity of assisting the Civilian Operation Commander or his/her Deputy

### **EUPOL COPPS**

- The HoM, in all cases foreseen by the Code of Conduct
- The Deputy HoM, in all cases foreseen by the Code of Conduct
- Mission members under disciplinary procedures
- Mission members appointed by the Responsible Authority as assessors (Article 12 of the Code of Conduct), as disciplinary investigators (Article 16 of the Code of Conduct), as members of a Disciplinary Board either as chairperson, as voting member or as non-voting secretary (Article 29 of the Code of Conduct) or as members of the Disciplinary Board of appeal either as chairperson, as voting member or as non-voting secretary (Article 39 of the Code of Conduct)
- The victim of the alleged breach (Articles 5bis.5b, 15.2, 18.5, 28.4, 32.3, 40.5 of the Code of Conduct)
- The line manager of any Mission member reporting a possible breach of the Code of Conduct (Article 6 of the Code of Conduct)
- The line manager of the Mission member under disciplinary procedure (Articles 18, 23, 28, 32, 40 of the Code of Conduct)
- National contingent leaders, national point of contact or other person inside the mission providing assistance to the Mission member under disciplinary procedure (Article 21.3 of the Code of Conduct)

### **Other actors**

- The competent authorities (the authorities of the Seconding State or of a contributing Third State, the authorities of the EU Institution or of the EEAS, the authorities of the state of nationality, the authorities of the Host State, the

Seconding Authorities and the authorities of the state of nationality) informed according to Article 2 of the Code of Conduct

- The persons acting on behalf of the Seconding Authority (Articles 1, 8.b, 10, 12, 16, 18, 22, 23, 26, 27, 28, 34, 40, 41, 46 of the Code of Conduct)
- Persons outside the Mission or external lawyers providing assistance to the Mission member under disciplinary procedure (Article 21.3 of the Code of Conduct)

## 6. ACCESS, RECTIFICATION, ERASURE OF DATA: What rights do you have?

You have the right of access to your personal data and the right to correct your inaccurate, or incomplete personal data taking into account the purpose of the processing. The right of rectification can only apply to factual data processed and shall not adversely affect the rights and freedoms of others. Completion of personal data could be by means of registering a supplementary statement in the file.

Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. Efforts will be made that if deemed legitimate rectification or deletion requests would be implemented in general in 10 working days.

Special attention is drawn to the consequences of a request for erasure, in which case any trace to be able to contact you will be lost. For more detailed legal references, you can find information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. The EEAS and EUPOL COPPS may restrict the right of access, rectification or erasure among others to protect the interest of the implementation of the Code of Conduct. If you wish to exercise your rights or have questions concerning the processing of your personal data, please address it to

- The Conduct and Integrity Entity ([EEAS-CONDUCT-AND -INTEGRITY-ENTITY@eeas.europa.eu](mailto:EEAS-CONDUCT-AND -INTEGRITY-ENTITY@eeas.europa.eu))
- EUPOL COPPS [data-protection@eupolcopps.eu](mailto:data-protection@eupolcopps.eu)

## 7. LEGAL BASIS: On what grounds we collect your data?

The processing of personal and disciplinary data when implementing the Code of Conduct is necessary for the performance of a task carried out by EUPOL COPPS and the European External Action Service and in particular for the management and functioning of the Missions and of the EEAS (Article 5(1)(a) of Regulation (EU) 2018/1725 as referred to in Recital 22 thereof and section 8.5 (a) of the Standard Operating Procedure on data protection for CSDP missions),

Legal references:

- 2010/427/EU Council Decision of 26/07/2010 establishing the organisation and functioning of the European External Action Service (OJ L 201)
- Code of Conduct and Disciplinary Procedure for EU Civilian CSDP Missions, as adopted by the Foreign Affairs Council on 16 December 2024 (Council document 16062/24), in particular Article 45 thereof
- Civilian Operation Commander instruction 28-2024 on the Code of Conduct and Disciplinary Procedure for Civilian CSDP Missions
- Council Joint Action 2005/797/CFSP of 14 November 2005 and its subsequent amendments
- OPLAN of EUPOL COPPS
- Civilian Operation Commander instruction 12-2018 on Standard Operating Procedure on personal data protection, and its subsequent amendment(s)
- Guidelines on data protection for CSDP Missions prepared by the EEAS Data Protection Office, the EEAS Civilian Planning and Conduct Capability and the EEAS Legal Affairs Division (Ares (2018)5161170) of 8 October 2018
- EUPOL COPPS' Standard Operating Procedure on Personal Data Protection

## 8. TIME LIMIT - DATA STORING: For what period and how we process your data?

### Retention periods:

- All cases that are either closed without further action or dealt with as a management issue right after the report concerning a possible breach of the Code of Conduct, are kept for a period of **two years** as of the decision by the Responsible Authority to close the case with or without management issue (Article 11.1.a) and b))
- All cases that are either closed without further action or dealt with as a management issue after a preliminary assessment of facts (without recourse to a disciplinary investigation) are kept for a period of **five years** as of the decision by the Responsible Authority to close the case with or without a management issue (Article 15 referring to Article 11.1.a) and b))
- All cases that are either closed without further action or dealt with as a management issue on basis of a disciplinary investigation report without having been submitted to a Disciplinary Board, are kept for a period of **ten years** as of the decision of the Responsible Authority (Article 28.1.a or b))

- All cases that are either closed without further action or dealt with as a management issue after the advice of a Disciplinary Board (irrespective of whether the advice is followed by the Responsible Authority) are kept for a period of **fifteen years** as of the decision of the Responsible Authority (Article 32.1.)
- All cases that are either closed without further action or dealt with as a management issue after the advice of a Disciplinary Board of appeal (irrespective of whether the advice is followed by the Responsible Authority) are kept for a period of **fifteen years** as of the decision of the Responsible Authority on appeal (Article 40)
- All cases where a written warning (Article 33 a)), a reduction of the salary by up to 30% for a period of maximum 3 months (Article 33 b)), a suspension without salary and allowances for a period of maximum three months (Article 33 c)), a non-renewal of contract (Article 33 d)), a non-extension of a tour of duty (Article 33 e)), a termination of the employment contract (Article 33 f)), a repatriation (Article 33 g)), a cooling off from CSDP Missions for a period of maximum three years (Article 33 h)) or a termination of appointment (Article 33 i)) has been taken as a disciplinary measure or as a recommendation of a disciplinary measure, are kept for a period of **twenty years** as of the decision of the Responsible Authority (Articles 32 to 34bis)
- All cases on appeal where written a warning (Article 33 a)), a reduction of the salary by up to 30% for a period of maximum 3 months (Article 33 b)), a suspension without salary and allowances for a period of maximum three months (Article 33 c)), a non-renewal of contract (Article 33 d)), a non-extension of a tour of duty (Article 33 e)), a termination of the employment contract (Article 33 f)), a repatriation (Article 33 g)), a cooling off from CSDP Missions for a period of maximum three years (Article 33 h)) or a termination of appointment (Article 33 i)) has been taken as a disciplinary measure or as a recommendation of a disciplinary measure, are kept for a period of **twenty years** as of the decision of the Responsible Authority on appeal (Article 40).

#### **Specific rules:**

In case the decision is challenged or in the event of a request or an inquiry (audit, investigation) by relevant authorities; in case of questions, claims or complaints by data subjects or other concerned individuals; personal and disciplinary data will be preserved as long as the legal claims arise, pending cases are ongoing or any follow-up action is due. This includes complaints, inquiries, pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. The personal and disciplinary data shall, however, be kept no longer than 5 years after the judgment on the pending case is final, respectively two years after a case before the European Ombudsman and its follow-up is closed.

At the expiration of the retention periods, the case files will be archived in a separate compartment, with an elimination of personal and disciplinary data if technically and reasonably feasible.

Data is intended to be kept for statistical purposes, in an anonymised form to the extent possible, taking into account the feasibility of the appropriate technical measures.

#### **Security of data:**

Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725.

- In its electronic format data will be stored in a cloud located within the EU. The collected personal and disciplinary data are processed by assigned staff members. Files have authorised access.
- Security is also ensured by the safety measures built in the various IT applications used
- Measures are provided by DIGIT/EEAS department and EUPOL COPPS CIS department to prevent non responsible entities from access, alteration, deletion, disclosure of data.

#### **9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?**

In case you have queries with regard to the data processed by the EEAS, you can contact the EEAS Data Protection Officer at [data-protection@eeas.europa.eu](mailto:data-protection@eeas.europa.eu).

In case you have questions or concerns related to the processing of your personal data by EUPOL COPPS, you can also contact the Mission Data Protection Advisor (MDPA) - Legal Adviser - at the functional mailbox of EUPOL COPPS [data-protection@eupolcopps.eu](mailto:data-protection@eupolcopps.eu).

#### **10. RECOURSE**

You have at any time the right to have recourse if you consider that your rights have been infringed as a result of the processing of your personal data. You may send your complaint to Mission Data Controller (the HoM of EUPOL COPPS) with the Mission Data Protection Advisor (MDPA) Legal Adviser in copy.

Concerning to the data processed by the EEAS you have at any time the right of recourse to the European Data Protection Supervisor at [edps@edps.europa.eu](mailto:edps@edps.europa.eu) after your question has been treated by the EEAS Data Protection Officer.