EUPOL COPPS Privacy Statement

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO MEDICAL DATA
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 overall objective of the processing activities covered by this Privacy Statement is to ensure that the duty of care is properly discharged in EUPOL COPPS, and to uphold that Missions Members (MMs) are safe and accounted for.

3. DATA PROCESSED

Data (category or type of data), including personal data, processed are the following:

Personal data:
- surname(s) and middle name(s) and first name(s)
- date and place of birth
- gender
- nationality(s)
- country of birth and place of birth
- home address (residence)
- insurance reference number
- mission id number
- personal phone details
- mission phone
- mission e-mail
- blood type
- medical opinions (reports from General Practitioner, Medical Specialists, Medical expertise, Hospitalisation reports, Medical Advisor, Psychologist)
- sick leave certificates
- individual medical files
- vaccination certificate
- pregnancy confirmation certificates
- medical data included in Fit to Work Certificate and other pre-deployment documents

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

Based on assessing risks related to potential access to data with regard to the process, the Mission ensures that adequate organisational and technical measures are in place in order to safeguard personal data of data subjects.
I. Organisational measures:
Confidentiality Declarations are to be signed by staff members dealing with medical information. Confidentiality acknowledgment is signed by all staff member who may have access to medical information (HR personal, CIS officers).
Access rights are granted strictly only to those personnel necessary to carry out their duties. Access to the data is limited to authorised personnel and it is subject to a password.

II. Technical measures:
Physical security is guaranteed by locked cupboards and locked premises.
Electronic security is guaranteed by access-protected files on Medical Adviser's computer. There are no shared drives or folders.
The evacuation authorisation is sent via ARES to the appropriate persons only AND there is a "lock" on the information which is called "medical secret" meaning that no one else can open this file in ARES than the persons it is send to.

Electronic Files:
Collected personal medical data is stored on Medical Adviser's personal computer. Access to personal medical data is only granted to Medical Adviser and any access is only allowed by means of Username and Password;

Physical Files:
Physical copies of the collected personal data are stored in a properly secured and locked storage cabinet.

4. CONTROLLER OF THE PROCESSING OPERATION
The Controller determining the purpose and the means of the processing operation is EUPOL COPPS. Mission’s Medical Advisers are responsible for managing the personal data processing operation which is under the supervision of the Head of Mission Nataliya Apostolova.

5. RECIPIENTS OF THE DATA
Medical data can be accessed only:

- Head of Mission in specifically defined cases.
- Medical Adviser. Medical Adviser provides the advice to the Human Resources and Mission Management on matters related to the medical condition of Mission Members. However, the Medical Adviser cannot disclose exact diagnosis to the Human Resources or Mission Management. The advice needs to be generic, formulated based on the medical data available to the Medical Adviser. In case the Medical Adviser needs more information to prepare the advice, additional data can be requested from the particular Mission Member.
- Dedicated members of the Mission in case of administrative aspects (HR, Finance Unit, Verification Officer).
- Legal Adviser in cases related to legal proceedings, repatriation or medical evacuation.
- Relevant staff of the CPCC and contracted legal advisors in case of legal proceedings.
- Mission/CPCC internal investigato rs, appointed by and acting on instructions of the relevant Mission/CPCC authority in disciplinary or security matters. In this case, only the information on sick leave can be shared without revealing the diagnosis.
- CIGNA or other insurance company in cases defined in the insurance contracts.

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:
- OPLAN
- Civilian Operations Commander Instruction 12/2018 on the SOP on Personal Data Protection
- Civilian Operations Commander Instruction on Medical clearance procedure for international contracted staff of civilian CSDP Missions
- SOP on Personal Data Protection
8. **TIME LIMIT FOR STORING DATA**

Medical files are retained for 30 years after the end of Mission of the concerned Mission member.

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. **RECOUSE**

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.