EUROPEAN UNION CAPACITY BUILDING MISSION PRIVACY STATEMENT – DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING MEDICAL DATA

1. INTRODUCTION

The protection of your privacy including your personal data is of great importance to the European Union and to EUCAP Mission. When processing personal data we reflect the principles of the Charter of Fundamental Rights of the European Union, and in particular the Article 8 on data protection.

This privacy statement describes how the EUCAP Mission processes your personal data for the purpose it is collected and what rights you have as a data subject.

Your personal data by the EUCAP Mission is processed in accordance the CivOpsCdr instruction 12-2018 and its subsequent amendment(s) on the SOP on the Protection of Personal Data for CSDP Missions by the CSDP Missions and in line 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 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), and repealing directive 95/46/EC.

All data of personal nature - data that can identify you directly or indirectly - is handled with the necessary care and according with the rules above.

2. PURPOSE OF THE PROCESSING: Why we process your data?

The purpose of processing your medical data is to provide appropriate medical and physiological support and advice to Mission members during the employment or assignment of local contracted, international contracted and seconded Mission members. This is to comply with the Mission's obligations and Head of Mission's duty of care, and to guarantee the Mission member's rights, in particular the right to the protection of personal data.

3. DATA PROCESSED: what data we process?

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

- surname(s), middle name(s) and first name(s);
- sex;
- date and place of birth (city, state);
- nationality, including multiple nationalities;
- home address (place of permanent residence);
- insurance reference number (Cigna) and insurance starting and ending dates;
- mission ID number;
- business and personal phone details;

- business and personal e-mail addresses;
- blood type;
- medical opinions (reports from general practitioner, medical specialist, medical expertise, hospitalization reports, medical advisor, psychologist) related to fitness to work or to any kind of medical incident or sickness;
- sick leave certificates;
- individual medical files regarding medical advise;
- vaccination certificates;
- supporting documents for certain kind of leaves (i.e. certificate stating the heath condition of the close relative);
- other background information, as appropriate.

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

The Controller determining the purpose and the means of the processing activity is Mission, represented by its Head of Mission. The Mission section responsible for managing the personal data processing is SECURITY AND DUTY OF CARE DEPARTMENT, under the supervision of the Head of Mission.
Medisoft Dossier Manager will process your data in a need to know bases in connection to develop and maintain the IT software.

5. RECIPIENTS OF THE MEDICAL DATA: Who has access to your data?

The recipients of the data are the following, on a strict "**need-to-know**" basis:

- Mission Medical personnel – all data;
- The health insurance provider of EUCAP Mission (Cigna) – all data;
- Investigator and responsible authorities involved in/with disciplinary proceedings, in a case of a need and in a specific single case, but limited to administrative information (no access to medical data);
- CPCC medical personnel based on the decision of Mission Medical personnel;
- Account manager(s) of the Medisoft Dossier Manager, in case of strict need for maintenance and development, no right to enter, alter or delete any data.

Transferring personal data to a third country (Host country)
Personal data is not intended to be transferred to a third country except for the purposes outlined below:
- a limited number of medical data of local contracted EUCAP Mission members may be shared with Host countries authorities for official, legitimate and lawful purposes, such as ensuring the payment of entitlements,

Transferring personal data to a third party
The given information will not be communicated to third parties, except where necessary for the purposes outlined below:
- upon request, the auditors might be provided with administrative health data for auditing purposes such as verification of payments based on medical certificate.

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

You have the right to access your personal data and the right to request for correction of 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 one month after your written request. If you have any queries or concerns related to the processing of your personal data, you may address them to the following functional mailbox: **data-protection@eucap-som.eu**

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

- Council Decision (CFSP) 2022/2445 of 12 December 2022 amending Decision 2012/389/CFSP on the European Union Capacity Building Mission in Somalia (EUCAP Somalia.)
- Revised Operational Plan, EEAS (2022) 1894 of 15/11/2022.
- Civilian Operations Commander Instruction 12/2018 of October 2018 on the Standard Operational Procedures (SOP) on Personal Data Protection.
- Mission Privacy Statement on Personal Data Protection (published on the Mission's website.)
- Civ Op Cdr instruction on the medical clearance procedure for contracted staff
  Other place holder (selection procedure.)

The processing is needed for reasons of substantial public interest: the execution of the Mission mandate and Head of Mission's duty of care for security and human resources administration during the employment/assignment as well as to ensure continuity of health care of the patients.

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

Retention period of medical data:

- In case of recruitment all medical data is kept and might be processed while the mission member is serving in the mission.
- In case of non-recruitment, the medical data will be kept for 2 years.
- Medical files are kept for 30 years after the mission member's end of mission.
- Sick leave certificates / notifications for Human Resources administration purposes are kept also according to the rules applicable to those purposes.

Outline of security measures:

- Electronic files will be stored in Medisoft Dossier Manager IT tool (soft copies): the collected medical data will be stored on servers, located in the Netherlands that abide by appropriate security rules. Assigned mission members will process medical data which are described under point 5. Files will have only authorized access. Measures are provided to prevent non-responsible entities from accessing the data. The system is ISO27001 certified.

- Physical files (hard copies): when not in use, physical copies of the collected medical data will be stored in a properly secured and locked storage container, e.g. filling cabinet or safe.

Technical and organizational 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 unauthorized person from gaining access to computer systems. Any unauthorized reading, copying; alteration or removal of storage media; any unauthorized memory inputs; any unauthorized disclosure, alteration or erasure of stored medical data; unauthorized persons from using data-processing systems by means of data transmission facilities;
- ensure that authorized users of a data-processing system can access no health data other than those to which their access right refers; the possibility to check logs; and that medical data being processed on behalf of third parties can be processed only upon instruction of the controller; furthermore that, during communication or transport of medical data cannot be read, copied or erased without authorization;
- record which medical data have been communicated, at what times and to whom;
- in case of processing medical data, it is handled with the necessary care and **is not intended to be disclosed or shared with third parties without consent from its subject(s**), except in the cases described in point 5 and for vital interest of the data subject.

Destruction of medical data: the mission has established systems and procedures for the deletion and destruction of medical data after the expiry of the retention period. The system and procedure ensure that protection of medical data through permanent destruction, for instance secure deletion of electronic files and secure shredding or burning of physical files, including storage media for electronic files (e.g. hard disc, flash memory sticks).

9. MISSION DATA PROTECTION ADVISOR: Any questions to the MDPA

In case you have questions or concerns related to the protection of your personal data, you can also contact the Mission Data Protection Advisor (MDPA) - Legal Adviser - at the functional mailbox of the EUCAP Mission: **data-protection@eucap-som.eu**

10. RIGHT TO HAVE 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 Head of the **EUCAP Mission**) with the Mission Data Protection Adviser (MDPA) Legal Adviser in copy.