EUCAP SOMALIA 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 the EUCAO Somalia 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 EEAS/CPCC and the EUCAP Somalia Mission processes your personal data for the purpose it is collected and what rights you have as a data subject.

The EUCAP Somalia process your personal data in accordance the CivOpsCdr instruction 17-2018 for CSDP Missions and its subsequent amendment(s) on the SOP on the Protection of Personal Data 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 in accordance 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. 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.

The overall objective of the processing activities covered by this Privacy Statement is to ensure that the duty of care is properly discharged and accounted for in all civilian CSDP Missions, and to uphold that Missions Members (MMs) are safe.

The Medical Team is bound by medical confidentiality.

Medical data is processed via the MediSoft IT system. Candidates and Mission Members will upload their own data. The medical adviser of the Missions and a limited number of other personnel, as elaborated in point 11, have access to the data on a strictly need to know basis. Medical data of data subjects may be processed for the following purposes:

1. Fit to work clearance for international contracted staff

The Fit to work clearance procedure is a medical procedure aiming to assess whether a selected candidate for an international contracted position in a civilian CSDP Mission is healthy and can perform a specific job or task, without being a hazard to him/herself and/or to others. International contracted Mission Members must comply with the Fit to work clearance procedure also during their term in the Mission. The Mission Members' medical data will be processed by the Mission's Medical Team, or, in case the Mission's Medical Advisers do not agree with a Fit to work clearance issued by the candidates own doctor, (also) by the CPCC Medical Team. Some seconding authorities adhere fully or partially to the Fit to work clearance procedures. Therefore, medical data of seconded personnel is also processed. The personal data provided either correspond to the full or the partial list of the data listed in point 9. There is no additional or other data collected.

2. Fit to work clearance for local staff

The Mission uses either (a) the Fit to work clearance procedure for international staff also for local contracted staff or (b) a less comprehensive clearance procedure. The personal data provided either correspond to the full or the partial list of the data listed in point 9. There is no additional or other data collected. All staff must provide their vaccination certificates to the Missions.

2. Consultation by Mission Medical Advisers

The purpose of keeping medical data of staff and of the consultation is to ensure the health and safety of all mission members and to identify health-related risks. Occasionally, on a case-by-case basis, the Mission's Medical Team may consult the CPCC Medical Team for example on health issue related to medical evacuation, relocation, return, departure/end of tour of duty/contracts of MMs and deployment of selected candidates as well as on heath conditions and/or ongoing treatments of both mission members and candidates.

3. DATA PROCESSED: what data we process?

Administrative data:

- Identification and contact data (name, nationality, age, place of origin, family status, phone & e-mail address.)
- Assignment-related data (date of deployment, relocations, end date of the tour of duty/contract, travel history.)

Medical data:

- Medical data included in the Medical Clearance Form (Annex to the Fit to work clearance procedure.)
- Individual medical files (general health information, specific medical conditions potentially giving rise to absence, risk factors, illnesses, medical incident, traumatic accidents, result of a health screening campaign.

Medical opinions (Reports from General Practitioner, Medical Specialists, Medical expertise, Psychologist; Hospitalisation report.) Medical and health related data in relation to COVID-19 pandemic situation (contamination and vaccination) and in particular data on the status of vulnerability.

Technical data

Time and modality of access in the logs.

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

The Controller determining the purpose and the means of the processing activity is the Civilian Operation Commander/Managing Director. The EUCAP Somalia is represented by the Head of Mission who is responsible for processing the personal data. The SECURITY AND DUTY OF CARE DEPARTMENT, under the supervision of the Head of Mission, is managing the data processing activities.

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

The recipients of the data are:

- The dedicated medical staff (medical advisers and nurses) of the EUCAP Somalia Mission,
- CPCC Medical Team (CPCC Medical Advisers/Coordinators) in the following instances:
  - if an individual is selected for a position before the Mission is established, or in a situation where the Mission's medical advisers disagree with a Fit to work report issued by the general practitioner of the data subject, or
  - in case of a medical evacuation, relocation, return, departure/end of tour of duty/contracts of MMs and deployment of selected candidates, or
  - when the CPCC Medical Team are consulted by medical advisers on heath conditions and/or ongoing treatments by the medical advisers in the Mission, or
  - when the CPCC Medical Team is de fact the Mission's medical adviser while a new Mission is being established,
  - when the CPCC Medical Team are de facto acting as a Mission's medical adviser because the Mission's medical adviser position is vacant, or the Mission's medical adviser is not capable to fulfil his/ her duty.

The data collected may, in duly justified cases, and on a need-to-know basis only, be shared with:

- The Civilian Operation Commander and the Head of Mission as per the Fit to work procedure.
- The EEAS Medical Team or other medical doctor assigned by CPCC for consultation during the Fit to work clearance procedure via MediSoft IT tool.
- Health insurance company providing health care service for civilian CSDP Missions - only in case of medical evacuation.
- MediSoft employees (the MediSoft Dossier Managers) if access is strictly needed for maintenance and development, and/or to investigate and solve issues flagged by the users. Medisoft employees will not have access to individual files, and thus cannot alter, delete or otherwise manipulate the data.

The medical data provided will not be communicated to third parties, except in the following cases and when in the interest of the person concerned:

- To the dedicated medical experts assigned by the seconding authorities upon their explicit request.
- To medical service providers (for example hospitals) where the person concerned is treated or about to be treated in case of referral.
- Other medical doctor assigned by CPCC for consultation during the Fit to work clearance procedure.
- Logs may be analysed by administrative or technical staff or staff of organisational entities and bodies charged with audit, inspection or investigative tasks in accordance with procedures of EU institutions or Union or member state law.

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: **medical@eucap-som.eu**

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

The processing of personal data, including health-related information is necessary for the performance of a task carried out by the missions 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 CPCC missions], and, in particular in the case of a medical evacuation, to protect the vital interest of the data subject [Article 5(1)(e) of Regulation (EU) 2018/1725 and section 8.5 (e) of the Standard Operating Procedure on Data Protection] and its processing is lawful pursuant to Article 10.2 (b),(c), (g) and (h) as well as to Art. 10.3 of Regulation (EU) 2018/1725.

Legal references, EUCAP Somalia:

- Council Decision: (CFSP) 2022/2445 of 12 December 2002
- Operational Plan: 14803/22 of 15 N5/11/2022
- CivOpCdr instruction 09-2021 on the medical procedure for international contracted staff of civilian CSDP Missions
- CivOpCdr instruction 05-2022 on the selection procedure for international contracted staff

Legal References, the EEAS:

- 2010/427/EU Council Decision of 26/07/2010 establishing the organisation and functioning of the European External Action Service (OJ L 201)
- Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385.)

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

Retention period of medical data:

- For Mission Members medical data collected in the context of the Fit to work procedure and occasionally, on a case-by-case basis are kept for 30 years after the termination of the contract/tour duties of the person concerned.
- For non-recruited candidates the data will be kept for 5 years or as long as the legal claims arising from the non-recruitment expire or any follow-up action is due.

Retention periods necessary for specific medical documents can be considered on a case-by-case basis. The retention periods could be also determined in relation to the nature of the respective document and the necessity to keep the particular data. No information or document is held more than 30 years after the termination of the contract/tour of duties of the person concerned unless the conditions in the next paragraph apply.

In case of an incident, extraordinary event or of an inquiry (audit, investigation) by authorities, questions, claims or complaints by data subjects or other concerned individuals' personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. The personal data shall, however, be kept not longer than 5 years after the judgment on the pending case is final.

Logs are kept as long as long as the data accessed is kept in MediSoft. 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.

Outline of security measures:

- Electronic files will be stored in MediSoft 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. Access to specific files requires authorization. Measures are provided to prevent non-responsible entities from accessing the data. The system is ISO27001 certified. MediSoft is surveyed by "Autoriteit Persoonsgegevens", the Dutch Data Protection Supervisor authority. The system is ISO27001 certificated. The developers work in conformity the guidelines in OWASP.

- 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 implemented according to Article 33 of Regulation (EU) 2018/1725 on data protection for EU institutions and bodies in order to:

- prevent any unauthorized person from gaining access to computer systems. This includes 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; and that medical data being processed on behalf of the EEAS and the Mission (the controller) by 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 and provide the possibility to check these logs.
- 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, e.g. hard disc, flash memory sticks, and secure shredding or burning of physical files.

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

In case of questions or concerns regarding protection of your personal data by CPCC.5, you may to contact the CPCC5-SECURITY-AND-DUTY-OF-CARE@eeas.europa.eu.

In case of questions or concerns regarding protection of your personal data by the Mission, you may to contact the Mission Data Protection Advisor (MDPA) at the functional mailbox: **data.protection@eucap-som.eu**

10. RIGHT TO RECOURSE

If you consider that your rights have been infringed as a result of the processing of your personal data, you have the right to recourse. For data processed by CPCC.5 you may send your complaint to the Mission Data Controller (the Head of Mission) with the Mission Data Protection Adviser (MDPA) in cc. See address above.