



EUROPEAN UNION CAPACITY BUILDING MISSION SOMALIA

PRIVACY STATEMENT ON MEDICAL DATA

I. LEGAL BASIS AND SCOPE:

The protection of your privacy including your personal data is of great importance to the European Union and to European Union Capacity Building Mission (EUCAP) in Somalia. 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 EUCAP SOMALIA processes your personal data for the purpose for which it is collected and what rights you have as a data subject. Your personal data is processed by the EUCAP SOMALIA in accordance with Regulation (EU) 2018/ 1725 of the European Parliament, 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 (repealing Regulation (EC) No 45/2001), Decision No 1247/2002/EC of 11 December 2018, aligned with provisions of the General Data Protection Regulation (EU) 2016/679 and in accordance with the CivOpsCdr instruction 12-2018 and subsequent amendments to the SOP on the Protection of personal data for CSDP Missions.

All data of personal nature which potentially can identify individuals directly or indirectly is processed fairly for specified purposes and in accordance with the law.

II. PURPOSE: Why we process your data?

The main purpose of processing medical data is to enable the Mission to provide medical advice/ treatment and psychological support to the Mission Members during their tour of duty/contract period.

III. DATA PROCESSED: What data we process?

The data, including personal data, which may be processed¹ includes the following information:

- surname(s), middle and first name(s)
- date and place of birth
- gender
- nationality
- country and place of birth
- home address (residence)
- insurance reference number
- mission ID number
- phone numbers and email addresses
- blood type
- various agreements/attestations/certifications/evaluations/declarations:
 - medical questionnaire
 - medical clearance form (fit for duty)

¹ While this list may not be exhaustive it includes most of the relevant and standard documents processed.

- vaccination certificates
- sick leave certificates and medical reports (GP, Specialist, Hospital)
- pregnancy confirmation certificates

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

Data Controller: EUCAP Somalia, represented by the Head of Mission, Christopher Reynolds.

V. ACCESS: Who has access to your data?

The Head of Mission, the Deputy Head of Mission, Medical staff, the SMSO as appropriate and in medical emergencies relevant senior mission managers.

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

You have the right to access your medical data, including to request correction of any inaccurate or incomplete personal data. In the unlikely event it is unlawfully collected you may request it is deleted.

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

- Council Decision: Counsel Joint Action 2008/796/CFSP and subsequent amendments latest Counsel Decision (CFSP) 2016/2238
- The OPLAN EEAS (2018) 1178
- CivOpsCom Instruction 12/2018 - SOP on Personal Data Protection
- EUCAP SOM - SOP on Personal Data Protection 17/07/2019
- The Status Agreement between the Federal Republic of Somalia and the European Union/EUCAP Somalia – 11/01/2020
- The Human Resource Handbook 2017

VIII. DATA STORAGE AND SECURITY: How is it organised?

As a general rule all data is stored electronically and is solely available to authorized mission staff. All data is stored and retained in accordance with the law and regulations, including the EUCAP SOP on Personal Data Protection.

Data are stored and secured in:

- Electronic format: the data will be stored on the Mission's servers that abide by the pertinent security rules. Personal data will be processed by assigned staff members. Files have authorised access. Measures are provided to prevent non-responsible entities from accessing data. General access to collected personal data and related information is only possible by duly authorized and accredited staff.
- Physical Files: When not in use physical copies of the collected personal data will be stored in a properly secured lockers and safes.

Specifically, appropriate technical and organisational measures apply:

- to ensure that authorised users can only access personal data relevant to their function and within their accreditation (access rights.) The possibility to check logs and access personal data potentially being processed on behalf of third parties can be processed only on instruction of the controller. Furthermore, during transfer of personal data the data cannot be read, copied or erased without authorization;
- to record which personal data have been communicated, at what times and to whom;
- to prevent any unauthorised individual(s) from gaining access to computer system, including unauthorised reading, copying, alteration or removal of storage media, as well as, any unauthorised memory inputs, unauthorised disclosure, alteration or erasure of stored personal data and to prevent unauthorised persons from using data-processing systems by means of data transmission facilities.

IX. RETENTION PERIOD: How long is data retained?

As a general rule Mission Members medical data will be retained for 30 years after termination of duties. However, five years after termination of duty medical data will be moved to a separate drive accessible only to HOM and the CPCC Chief Medical Officer. In case of Mission closure such medical data will be

archived with the EEAS Information and Document Management Sector.

For non-selected candidates the medical data is retained for two years after completion of the relevant Call for Contribution after which it is permanently deleted.

In cases involving litigation or a complaint the medical data will be retained for 5 years after the final decision/judgment is rendered.

After the expiry of the respective retention periods all medical data (electronic and hard copy) will be permanently deleted by shredding, burning or erasure of all data storage.

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

In case you have questions related to the protection of your medical data please contact the Missions Data Protection Advisor (MDPA) on: data-protection@eucap-som.eu

XI. RECOURSE

You have at any time the right of recourse by addressing a request or complaint in writing to the HOM of EUCAP SOMALIA.