European Union Advisory Mission in Iraq

PRIVACY STATEMENT

regarding the processing and protection of personal medical data

1. **Introduction:** What is this statement about?

Personal data is data that can identify you as a person, directly or indirectly. The protection of your privacy including your personal data is of great importance to the European External Action Service (EEAS) and its Civilian Planning and Conduct Capability (CPCC) directorate, the European Commission's Service for Foreign Policy Instruments (FPI), and the civilian crisis management missions under the European Union's Common Security and Defence Policy (CSDP) including the European Union Advisory Mission in support of Security Sector Reform in Iraq (EUAM Iraq). Consequently, all personal data that can identify you either directly or indirectly will be handled legitimately and with the necessary care. When processing personal data, EUAM Iraq respects the principles of the Charter of Fundamental Rights of the European Union, especially its Article 8 on data protection.

This Privacy Statement describes how EUAM Iraq processes your personal data for the purpose for which it has been or is going to be collected and what rights you have as a data subject.

Your personal data is collected, processed, and stored by EUAM Iraq in accordance with the principles and provisions of the applicable legislation on data protection, including the Regulation (EU) 2018/1725 of 23 October 2018 of the European Parliament and of the Council 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, aligned with the provisions of the Regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the General Data Protection Regulation, GDPR), and in accordance with the Civilian Operations Commander's Instruction no. 12 of 2018 and its subsequent amendments as well as with EUAM Iraq's Standard Operating Procedures (SOP) no. 21 of 24 February 2019 on Personal Data Protection.

All data of personal nature is handled with the necessary care.

2. **Purpose of the data processing operation:** Why do we process your personal data?

The purpose of processing your medical data is to provide appropriate medical and physiological support and advice to mission members (MMs) during the deployment of seconded MMs or employment of internationally or locally contracted MMs. This is to comply with the Mission's obligations and the Head of Mission's duty of care, and to guarantee the MMs' rights, especially the right to the protection of personal data.

3. **Data that has been or will be processed:** What personal data do we process?

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

1. Surname(s), middle name(s) and first name(s);
2. Sex;
3. Date of birth;
4. Nationality, including multiple nationalities;
5. Home address (place of permanent residence);
6. Insurance reference number and the insurance's commencement and ending dates;
7. Mission identity card number;
8. Business and personal phone details;
9. Business and personal email addresses;
10. Blood type;

11. Medical opinions (reports from general practitioner, medical specialist, medical expertise, hospitalisation reports, medical advisor, psychologist) related to fitness to work or to any kind of medical incident or sickness;
12. Sick leave certificates;
13. Individual medical files regarding medical advice;
14. Vaccination certificates;
15. Supporting documents for certain kinds of leave, e.g. certificate stating the health condition of close relatives;
16. Other clinical background information, as appropriate:
    a. Partner's (or authorised person's) name and contact details;
    b. Body identifying marks, e.g. scars, tattoos;
    c. Medical history and conditions including pharmaceuticals/medicine;
    d. Allergies;
    e. Drinking and smoking status;
    f. Body Mass Index (BMI); and,
    g. Data collected during medical health campaigns, e.g. lung peak expiratory flow and cholesterol; and,
17. Mission entity to which the Data Subject is assigned, e.g. division, department, section, unit, office or team.

4. Controller of the data processing operation: Who is entrusted with processing your personal data?

The controller determining the purpose and the means of the processing activity is EUAM Iraq, represented by its Head of Mission, which in this capacity executes his or her duty as Data Controller. The Mission entity responsible for managing the collection and processing of medical data and the relevant database is the Mission's Medical Section, which is an entity under the Security and Duty of Care Department (SDCD) under the supervision of the Head of Mission.

The Medisoft dossier manager will process your data on a need-to-know basis in connection with developing and maintaining the software.

5. Recipients of the data: Who has access to your personal data?

The recipients of your data may include the following:

I. Within the Mission:
    a. All Medical Section personnel has access to all information in the Medisoft database.
    b. Investigators and authorities involved in disciplinary proceedings, if needed and in specific cases, but limited to administrative information, i.e. no access to medical data.

II. Outside of the Mission:
    a. Medical personnel of CPCC.
    b. Personnel of the Mission's health insurance provider (currently Cigna).
    c. Account manager(s) of the Medisoft dossier manager, if strictly needed for maintenance and development, and with no right to enter, alter or delete any data.
    d. Relevant public authorities of Iraq, EU, EU member states or contributing third states involved in disciplinary or criminal proceedings or to fulfil other legal requirements, as applicable.
    e. A limited amount of medical data of locally contracted MM may be shared with authorities of Iraq for official, legitimate and lawful purposes, e.g. for ensuring the payment of entitlements.
    f. External auditors but only administrative data and only for auditing purposes, e.g. verification of payments based on medical certificates.

The personal data will not be communicated to third parties except where necessary for the purposes outlined above.

6. Provision, access, rectification and erasure of the data: What rights do you have?

You have the right to access your personal data and the right to request correction of any inaccurate or incomplete personal data. When applicable, for instance if your personal data have been collected illegally, you have the right to request erasure of the data, to restrict the processing of it, the right to data portability as well as the right to object to the processing, which is lawfully carried out pursuant to Article 5(1)(a) of Regulation EU 2018/1725 and Section 3.3 of the CIVOPSCDR's Instruction no. 12 of 2018 on grounds relating to your situation.

If you wish to exercise your rights or if you have any queries concerning the processing of your personal data, you may address them to the following functional mailbox: admin.medical@euam-iraq.eu.

7. Legal bases for the data processing operation: On which grounds do we collect your personal data?

We process your personal data because:

1. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body or the Mission; and/or,
2. Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, including but not limited to fulfil the Head of Mission's duty of care and the Mission's human resources management, and ensure continuity in the health care of MMs.

In particular, the applicable legal provisions are the following:

– Article 6 of the Foreign Affairs Council of the European Union's Decision no. (CFSP) 2017/1869 of 16 October 2017, as amended by Council Decisions (CFSP) 2018/1545 of 15 October 2018 and (CFSP) 2020/513 of 7 April 2020; and,

– Article 4.3.1 of the Mission's 2022 Operations Plan (OPLAN, RESTREINT UE/EU RESTRICTED).

8. Time limit for storing data: How long do we store your personal data?

I. Retention of data:

1. Personal data such as listed in Section 3 above will:
   a. Be kept and might be processed while the MM is serving in the Mission;
   b. In any instance, be retained for 30 years after the end of service of the respective mission member who has entered the data into the Mission's database, for the purpose of audit and possible investigation;
   c. In case of a judicial procedure related to employment of a contracted mission member or tour of duty of a seconded mission member, be kept for five (5) years after the final judgment was rendered; and/or,
   d. In case of a complaint launched before the European Ombudsman or before the European Data Protection Supervisor or an investigation conducted by the European Anti-Fraud Office (OLAF) or by the European Public Prosecutor's Office (EPPO) or a verification by the European Court of Auditors, be kept for five (5) years after the closure of the case.
2. Sick leave certificates and/or notifications for human resources management purposes are also kept according to the rules applicable to those purposes.

II. Security of data:

1. Appropriate organisational and technical measures are ensured as follows:
   a. Personal data will be stored in electronic format in a database (Medisoft), on servers located in the Netherlands and abiding to appropriate security rules. Assigned MMs will process medical data such as listed in Section 5 above. Files will have only authorised access. Measures are provided to prevent non-authorised entities or individuals from accessing the data. The system is ISO27001 certified.
   b. Physical files (hard copies): When not in use, physical copies of the collected medical data will be stored in properly secured and locked storage containers, e.g. filing cabinets or safes.
   c. Technical and organisational measures are also guaranteed according to the appropriate provisions on security of the successor regulation on data protection for EU institutions and bodies to ensure the following:
      (i) Prevent any unauthorised entities or individuals from gaining access to computer systems for any unauthorised reading, copying; alteration or removal of storage media; any unauthorised memory inputs; any unauthorised disclosure, alteration or erasure of stored medical data; or unauthorised use of data-processing systems by means of data transmission facilities.
      (ii) Authorised users of a data-processing system cannot access any health data other than those to which their access rights permit. The possibility to check logs and that medical data is being processed on behalf of third parties can be processed only upon instruction or authorisation of the Data Controller; furthermore, during communication or transport of medical data it cannot be read, copied or erased without authorisation.
      (iii) Record which medical data have been communicated, at what times and to whom.
      (iv) When processing medical data that it is handled with the necessary care and **is not intended to be disclosed or shared with third parties without consent from its Data Subject(s**), except in the cases described in Section 5 and for vital interest of the Data Subject.

III. Destruction of data:

The mission has established systems and procedures for the deletion and destruction of medical data after the expiry of the retention period, which ensure the 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 discs, flash memory sticks).

9. Data protection contact: Do you have any questions regarding this statement?
If you have queries regarding the protection of your personal data, you may also contact EUAM Iraq's Mission Data Protection Advisor (MDPA) at data.protection@euam-iraq.eu.
10. Recourse: Where can you complain?
You have at any time the right of recourse, which you may submit to EUAM Iraq's Data Controller with the MDPA in copy, via data.controller@euam-iraq.eu.

DISCLAIMER

This Privacy Statement is subject to adjustments in line with the completed internal data protection procedure arrangements of both the EEAS/CPCC, the Commission/FPI and the EUAM Iraq mission.