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 the EEAS/CPCC and 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.

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, including EUAM Iraq, and that MMs are safe.

The MMs of the Mission's Medical Section is bound by medical confidentiality.

Medical data is processed via the MediSoft Information Technology (IT) system. Candidates for vacant positions and MMs shall upload their own data. The Mission's Medical Adviser 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 procedure for international contracted MMs

The Fit-to-Work clearance procedure is a medical procedure for assessing whether a selected candidate for an international contracted position in a civilian CSDP mission, including EUAM Iraq, is healthy and can perform a specific job or task without being a hazard to him- or herself and/or to others. International contracted MMs shall comply with the Fit-to-Work medical clearance procedure during their term in the Mission as well. *A priori* medical data will be processed by the Mission's Medical Section. However, if someone is selected for a position before the Mission is established or the Mission's Medical Adviser does not agree with the opinion on the fitness provided by the general practitioner of the Data Subject, the CPCC Medical Team may also handle the medical data.

Some seconding authorities adhere fully or partially to the Fit-to-Work medical 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 Section 9. No additional data is collected.

2. Fit to work clearance for national contracted MMs

Missions either use the Fit-to-Work clearance procedure for intl. MMs for national contracted MMs or have introduced a less comprehensive clearance procedure. The missions will not process more data that those listed in this Privacy Statement.

All intl. MMs shall share their vaccination certificates with the Mission.

3. Consultation by Mission Medical Advisers

The purpose of keeping medical data of MMs and of the consultation is to ensure the health and safety of all MMs and to identify health-related risks.

Occasionally, on a case-by-case basis, the Mission's Medical Section may consult the CPCC Medical Team, for example on health issues 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 MMs and candidates.

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:

A. Administrative data

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; and,
10. Mission entity to which the Data Subject is assigned, e.g. division, department, section, unit, office or team.

B. Medical data

Medical data included in the Medical Questionnaire and Clearance Form (annexed to the Fit-to-Work medical clearance procedures), individual medical files (e.g. information about general health status, specific medical conditions giving rise to absence, risk factors, illnesses, medical or traumatic incidents, results of health screening campaigns), medical opinions (e.g. reports prepared by the MM's general practitioner, medical specialists or experts, psychologist, and/or hospital records), medical and health related data in relation to the COVID-19 pandemic (contamination and vaccinations), especially date on the status of vulnerability, and/or including but not limited to the following:

1. Blood type;
2. 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;
3. Sick leave certificates;
4. Individual medical files regarding medical advice;
5. Vaccination certificates;
6. Supporting documents for certain kinds of leave, e.g. certificate stating the health condition of close relatives;
7. 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.

C. Technical data

Time and modality of access to the logs.

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 the CIVOPSCDR/Managing Director of the CPCC whereas the EUAM Iraq mission, represented by its Head of Mission, 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), headed by the Senior Mission Security Officer who is under the supervision of the Head of Mission.

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 (the Medical Adviser, his or her deputy, nurses) have 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. not including access to medical data.

II. Outside of the Mission:

a. Medical personnel of CPCC (e.g. the CPCC Medical Adviser/Coordinator) if or when:

(i) A candidate is selected for a position before the Mission is established or the Mission's Medical Adviser does not agree with the opinion on the fitness provided by the Data Subject's general practitioner;

(ii) In case of medical evacuation, relocation, return, departure at end of tour of seconded deployment or expiry or termination of employment contracts of MMs and deployment of selected candidates;

(iii) Consulted by the Mission's medical staff on heath conditions and ongoing treatment by them;

(iv) They are acting as a new mission's medical adviser during its establishment; and/or,

(v) They are acting as a Mission's medical adviser when his or her position is vacant or the Mission's medical adviser is not able or capable to fulfil of his or her duties.

b. Members of the EEAS's medical team or a medical doctor assigned by the CPCC for consultation during the Fit-for-Work clearance procedure and only via the MediSoft application.

c. The CIVOPSCDR during the Fit-for-Work clearance procedure, only to a limited extent, only in writing, and only in duly justified cases.

d. Personnel of the Mission's health insurance provider (currently Cigna) and only in case of medical evacuation and only in writing, emails included.

e. MediSoft employees (MediSoft dossier managers), if strictly needed for maintenance and development and to investigate and solve issues raised or flagged by MediSoft users, and with no right to enter, alter or delete or otherwise manipulate any data. They shall only have access to rows of data needed to accomplish their tasks.

f. Dedicated medical experts assigned by the MMs' seconding authorities and only in response to their explicit request.

g. Medical service providers, e.g. hospitals, where the concerned MM is treated or is about to be treated in case of referral.

h. 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.

i. 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.

j. Administrative or technical staff of organisational entities charged with audit, inspection or investigation in accordance with procedures of EU institutions or Union or member state law.

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 concerns or queries regarding 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?

Your personal data is processed 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.

The processing of personal data, including health-related information, is necessary for the performance of a task carried out by the missions and the EEAS and in particular for the management and functioning of the missions and of the EEAS pursuant to Art. 5(1)(a) of Regulation (EU) 2018/1725 as referred to in Recital 22 thereof and Section 8.5(a) of the SOP 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 pursuant to Art. 5(1)(e) of Regulation (EU) 2018/1725 and Section 8.5(e) of the SOP on Data Protection, and its processing is lawful pursuant to Art. 10.2(b), (c), (g) and (h) and Art. 10.3 of Regulation (EU) 2018/1725.

In particular, the applicable legal provisions are the following:

For the Mission:

- Art. 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, (CFSP) 2020/513 of 7 April 2020 and (CFSP) 2024/1247 of 29 April 2024; and,
- Art. 4.3.1 of the Mission's 2024 Operations Plan (OPLAN, RESTREINT UE/EU RESTRICTED), available at the Mission's SDCD;
- The CIVOPSCDR's Instruction no. 9 of 24 March 2021 on *Medical Clearance Procedure for International Contracted Staff of Civilian CSDP Missions;* and,
- The CIVOPSCDR's Instruction no. 5 of 13 May 2022 on *Revised Selection Procedure for International Personnel of Civilian CSDP Missions*.

For the EEAS:

- Council Decision 2010/427/EU of 26 July 2010 *Establishing the Organisation and Functioning of the European External Action Service* (Official Journal (OJ) of the EU, J L 201); and,
- 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 of 14 June 1962, p. 1385).

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;
   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 and/or,
   e. For non-recruited applicants/candidates, the data will be kept for five (5) years or as long as any legal claims arising from the non-recruitment expire or any follow-up action is due.
2. Sick leave certificates and/or notifications for human resources management purposes are also kept according to the rules applicable to those purposes.
3. Retention periods necessary for specific medical documents may 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 specific data. No information or document will be kept more than 30 years after the termination of the employment contract or end of tour of seconding of the person concerned unless the conditions in the next paragraph apply.
4. In case of an incident, extraordinary event or an inquiry (audit, investigation, inquest) by authorities of competent jurisdiction, 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 decisions, rulings and judgments to allow for the exhaustion of all avenues of appeal and other channels of legal remedies. The personal data shall, however, be kept not longer than five (5) years after the judgment on the pending case is final.
5. Logs are kept as long as long as the data accessed is kept in the MediSoft database.
6. Data is intended to be kept for statistical purposes, in an anonymised form to the extent possible, considering the feasibility of the appropriate technical measures.

II. Security of data:

1. Appropriate organisational and technical measures are ensured as follows:
   a. Personal data will be stored in electronic format in the MediSoft database, 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. Access to specific files require authorisation. Measures are provided to prevent non-authorised entities or individuals 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 with OWASP[1] guidelines.
   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 implemented pursuant to Art. 33 of Regulation (EU) 2018/1725 on *Data Protection for EU Institutions and Bodies* to ensure the following:

[1] The *Open Worldwide Application Security Project* (OWASP) is an online community that produces freely available articles, methodologies, documentation, tools and technologies in the fields of *Internet of Things* (IOT), system software and web application security. See owasp.org.

(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) Ensure that 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, and provide the possibility to check the related logs.

(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 contact EUAM Iraq's Mission Data Protection Advisor (MDPA) at data.protection@euam-iraq.eu.

Queries regarding the protection of your personal data handled by the CPCC, you may contact the CPCC's Security and Duty of Care division via cpcc5-security-and-duty-of-care@eeas.europa.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.