European Union Advisory Mission in Iraq

PRIVACY STATEMENT

regarding the processing and protection of personal data during disciplinary proceedings

1. Introduction: What is this personal data protection notification/privacy 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 Union Advisory Mission in support of Security Sector Reform in Iraq (EUAM Iraq, the Mission). 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, the Mission 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 Mission 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, including disciplinary information, is collected, processed, and stored by the Mission 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 (CIVOPSCDR's) Instruction no. 12 of 2018 and its subsequent amendments as well as with the Mission'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 personal data is to implement the *Code of Conduct and Disciplinary Procedure for EU Civilian CSDP Missions,* hereinafter referred to as the Code. For the sake of clarity, the personal data in the context of the implementation of the Code is referred to as "disciplinary data".

The Code aims at guaranteeing a healthy and safe work environment in the Mission where all mission members can reasonably from their peers expect high personal standards of ethical behaviour, impartiality and integrity, as well as acting in an irreproachable manner during and outside working hours.

The CIVOPSCDR shall ensure that The European Union's duty of care is properly discharged. The Head of Mission (the HOM) is responsible for disciplinary control over the Mission's staff. The CIVOPSCDR and the HOM shall guarantee a safe and secure work environment for the Mission's personnel, considering the volatile environment where the Mission is deployed.

On 16 December 2024, the Council of the European Union approved the revised *Code of Conduct and Disciplinary Procedure for EU Civilian CSDP Missions* (the Code of Conduct), which includes measures to guarantee the impartiality and objectivity of investigations conducted by the Mission and by the Conduct and Integrity Entity established by the Code. Applying the Code involves by nature the processing of disciplinary data. The Code's Article 45 states, *"In the framework of this Code, personal data shall be collected only to the extent necessary and relevant and in accordance with the principles and procedures of personal data protection as contained, in particular, in the Civilian Operations Commander's Instruction no. 12-2018 for the Missions and in Regulation (EU) 1725/2018 for what concerns the EEAS"*.

Personal data will be processed when a mission member or a third party submits a report, during the preliminary assessment of facts and during disciplinary investigations, including appeals and the decisions of the respective responsible authority. Personal data may be collected for the purpose of providing evidence in documents, statements, observations, on-site inspections and interviews, both in electronic (emails, photo, screenshots etc.) and physical forms. The report of the breach and any further information collected during the preliminary assessment and/or investigations is kept in the case file. The case files are kept by the responsible authority.

The processing activity aims at rendering effective the Code's Article 45 by complying with all requirements foreseen by the rules on personal data protection.

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:

I. Administrative data

1. Identification data, for example:
   a. Surname(s), middle name(s) and first name(s);
   b. Sex;
   c. Date and location of birth;
   d. Nationality, including multiple nationalities;
   e. Staff category;
   f. Position within the Mission (job title);
   g. Mission entity to which the Data Subject is assigned, e.g. division, department, section, unit, office or team;
   h. Mission identity card number; and,
   i. Occupation for third parties concerned.
2. Contact data, for example:
   a. Business and personal (home) address (place of permanent residence);
   b. Business and personal phone details; and,
   c. Business and personal email addresses.
3. Any other personal data necessary for the case file.

II. Case file related data

1. All personal data processed by the Conduct and Integrity Entity when completing its tasks pursuant to the Code (Article 5bis of the Code);
2. All personal data included in the report (Article 6):
3. All personal data collected during the preliminary assessment of facts (Articles 12-15);
4. All personal data collected during the disciplinary investigation (Articles 16-20);
5. All personal data submitted to the Disciplinary Board and included in its written advice (Articles 29-31);
6. All personal data included in the decision of the Responsible Authority in the first instance (Articles 32-34):
7. All personal data included in appeals by the mission member under disciplinary procedure (Article 35);
8. All personal data submitted to the Disciplinary Board of Appeal and/or included in its written advice (Articles 39 and 40);
9. All personal data included in the decision taken by the Responsible Authority in the second instance (Article 40);
10. All personal data included in supporting document(s), e.g. correspondence with Member States on decisions taken by the Responsible Authority; and/or,
11. Any other personal data emerging from the implementation of the Code.

III. Specific data

1. Specific data refer to the data used to identify and to contact mission members appointed to a specific role in the framework of the Code (Responsible Authority, assessors, investigators, members of disciplinary boards and members of disciplinary boards of appeal), including but not limited to the following:
   a. Name and surname;
   b. Role in the framework of the Code; and,
   c. Contact data (email address and phone number).
2. The data may be processed for the following data subjects:
   a. Mission members under disciplinary proceedings:
      (i) Head of Mission;
      (ii) Members seconded by EU member states or contributing third states;
      (iii) Members seconded by EU institutions or the EEAS;
      (iv) International contracted mission members; or,
      (v) National (locally) contracted mission members.
   b. Mission members, staff of the EEAS or staff appointed by an EU member state in the roster, appointed to a specific role in the framework of the Code:
      (i) Responsible Authority;
      (ii) Assessor;
      (iii) Investigator; or,
      (iv) Member of a disciplinary board.
   c. Any other person involved or related to the fact(s), event(s) and/or behaviour(s) having led to the implementation of the Code, e.g. suspect, victim of the breach, witness, interviewee or provider of information or evidence.

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 HOM who in this capacity executes his or her duty as Data Controller.

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

The recipients of your data, on a strict need-to-know basis, may include the following:

I. Within the Mission:

1. The HOM in all cases foreseen by the Code;
2. The Deputy Head of Mission (DHOM) in all cases foreseen by the Code;
3. Mission members under disciplinary proceedings;
4. Mission members appointed by the Responsible Authority as assessors (Article 12 of the Code), as disciplinary investigators (Article 16), as members of a Disciplinary Board either as chairperson, as voting member or as non-voting secretary (Article 29) or as members of the Disciplinary Board of Appeal either as chairperson, voting member or non-voting secretary (Article 39);
5. The victim of the alleged breach (Articles 5bis.5b, 15.2, 18.5, 28.4, 32.3 and 40.5);
6. The line manager of any mission member reporting a possible breach of the Code (Article 6);
7. The line manager of the mission member under disciplinary proceedings (Articles 18, 23, 28, 32 and 40); and/or,
8. National contingent leaders, national points of contact or other person(s) inside the Mission aiding the mission member under disciplinary proceedings (Article 21.3).

II. Outside of the Mission:

1. The CPCC:
   a. The CIVOPSCDR in all cases foreseen by the Code;
   b. The Deputy CIVOPSCDR in all cases foreseen by the Code; and/or,
   c. Assigned advisors of the CPCC Managing Director and only on a need-to-know/need-to-do basis in their capacity as assisting the CIVOPSCDR or his or her Deputy.
2. The EEAS:
   a. Staff of the EEAS Conduct and Integrity Entity (MD.CPCC), given the tasks assigned to this Entity (Article 5bis of the Code);
   b. Experts from the roster referred to in Article 5bis and Annex I of the Code (EEAS experts, experts appointed by Member States and experts made available by Missions) appointed as the following:
      (i) Preliminary assessors (Article 12) by the Responsible Authority;
      (ii) Disciplinary investigators (Article 16) by the Responsible Authority;
      (iii) Members of the Disciplinary Board either as chairperson, as voting member or as non-voting secretary (Article 29); or,
      (iv) Members of the Disciplinary Board of Appeal either as chairperson, as voting member or as non-voting secretary (Article 39).

III. Other actors:

1. The competent authorities (the authorities of a mission member's seconding state or of a contributing third state, the authorities of the EU Institution or of the EEAS, the authorities of the state of nationality, the authorities of the host state, the seconding authorities and the authorities of the state of nationality informed according to Article 2 of the Code;
2. The persons acting on behalf of the mission member's seconding authority (Articles 1, 8(b), 10, 12, 16, 18, 22, 23, 26, 27, 28, 34, 40, 41 and 46); and/or,
3. Persons outside the Mission or external lawyers aiding the mission member under disciplinary proceedings (Article 21.3).

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 considering the purpose of the processing. The right of rectification can only apply to factual data processed and shall not adversely affect the rights and freedoms of others. Completion of personal data could be by means of registering a supplementary statement in the file.

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. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one (1) month from the receipt of your request. The period may be extended by two (2) further months if necessary. Efforts will be made that, if deemed legitimate, rectification or deletion requests would be implemented in general within ten (10) working days.

Special attention is drawn to the consequences of a request for erasure, in which case any trace to be able to contact you will be lost. For more detailed legal references, you can find information in Articles 14-21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. The EEAS and the Missions may restrict the right of access, rectification or erasure among others to protect the interest of the implementation of the Code.

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 institutional mailboxes:

The Mission: data.protection@euam-iraq.eu.

The Conduct and Integrity Entity: (EEAS-CONDUCT-AND-INTEGRITY-ENTITY@eeas.europa.eu).

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

Your personal data and of disciplinary data when implementing the Code is processed because:

1. Processing is necessary for the performance of a task carried out by the Mission and the EEAS and 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.

The processing of personal and disciplinary data is necessary for the performance of tasks carried out by the Mission and the EEAS and in particular for the management and functioning of the Mission and of the EEAS pursuant to Article 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 disciplinary proceedings, 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 for CSDP Missions, and its processing is lawful pursuant to Articles 10.2(b), (c), (g) and (h) and 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 Security and Duty of Care Department (SDCD).

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);
- *Code of Conduct and Disciplinary Procedure for EU Civilian CSDP Missions,* as adopted by the Foreign Affairs Council on 16 December 2024 (Council document 16062/24), especially its Article 45.
- The CIVOPSCDR's Instruction no. 28 of 18 December 2024 on the *Code of Conduct and Disciplinary Procedure for Civilian CSDP Missions;*
- The CIVOPSCDR's Instruction no. 12 of 8 October 2018 on a *Standard Operating Procedure on Personal Data Protection* and its subsequent amendment(s);
- *Guidelines on Data Protection for CSDP Missions* prepared by the EEAS Data Protection Office, the CPCC and the EEAS Legal Affairs Division (Ares (2018)5161170) of 8 October 2018;
- The Mission's SOP no. 21 of 24 February 2019 on *Personal Data Protection;* 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 mission member is serving in the Mission;
   b. All cases that are either closed without further action or dealt with as a management issue right after the report concerning a possible breach of the Code are kept for a period of two (2) years as of the decision by the Responsible Authority to close the case with or without management issue (Code's Article 11.1(a) and (b));
   c. All cases that are either closed without further action or dealt with as a management issue after a preliminary assessment of facts without recourse to a disciplinary investigation are kept for a period of five (5) years as of the decision by the Responsible Authority to close the case with or without a management issue (Article 15 referring to Article 11.1(a) and (b));
   d. All cases that are either closed without further action or dealt with as a management issue on basis of a disciplinary investigation report without having been submitted to a Disciplinary Board are kept for a period of ten (10) years as of the decision of the Responsible Authority (Article 28.1(a) or(b));
   e. All cases that are either closed without further action or dealt with as a management issue after the advice of a Disciplinary Board irrespective of whether the advice is followed by the responsible authority are kept for a period of fifteen (15) years as of the decision of the Responsible Authority (Article 32.1);

f. All cases that are either closed without further action or dealt with as a management issue after the advice of a Disciplinary Board of appeal irrespective of whether the advice is followed by the responsible authority are kept for a period of fifteen (15) years as of the decision of the Responsible Authority in the appeal instance (Article 40);

g. All cases where a written warning (Article 33(a)), a reduction of the salary by up to 30 % for a period of maximum three (3) months (Article 33(b)), a suspension without salary and allowances for a period of maximum three (3) months (Article 33(c)), a non-renewal of employment contract (Article 33(d)), a non-extension of seconded tour of duty (Article 33(e)), a termination of employment contract (Article 33(f)), repatriation (Article 33(g)), cooling-off from CSDP missions for a period of maximum three (3) years (Article 33(h)) or a termination of appointment (Article 33(i)) has been taken as a disciplinary measure or as a recommendation of a disciplinary measure, are kept for a period of twenty (20) years as of the decision of the Responsible Authority (Articles 32-34bis); or,

h. All cases on appeal where a written warning (Article 33(a)), reduction of the salary by up to 30 % for a period of maximum three (3) months (Article 33(b)), suspension without salary and allowances for a period of maximum three (3) months (Article 33(c)), not offering a new employment contract (Article 33(d)), non-extension of seconded tour of duty (Article 33(e)), termination of employment contract (Article 33(f)), repatriation (Article 33(g)), cooling-off from CSDP missions for a period of maximum three (3) years (Article 33(h)) or termination of appointment (Article 33(i)) has been taken as a disciplinary measure or as a recommendation of a disciplinary measure are kept for a period of twenty (20) years as of the decision of the Responsible Authority on appeal (Article 40).

2. Specific rules:

a. If the Responsible Authority's decision is challenged or in the event of a request or an inquiry (audit, investigation) by authorities of competent jurisdiction, questions, claims or complaints by data subjects or other concerned individual, personal and disciplinary data will be preserved as long as the legal claims arising from the proceedings expire, pending cases are ongoing or any follow-up action is due. This may include complaints, inquiries, 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 and disciplinary data shall, however, be kept no longer than five (5) years after the final judgment was rendered.

b. 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, the personal and disciplinary data will be kept for five (5) years after the closure of the case.

c. At the expiration of the retention periods, the case files will be archived in a separate compartment, with an elimination of personal and disciplinary data if technically and reasonably feasible.

d. Data may 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 pursuant to Article 33 of Regulation (EU) 2018/1725 on *Data Protection for EU Institutions and Bodies* as follows:

a. In its electronic format personal and disciplinary data will be stored in a cloud located within the EU. The collected personal and disciplinary data are processed by assigned staff members. Files have authorised access.

b. Security is also ensured by the safety measures built into the various IT applications used.

c. Measures are provided by the DIGIT/EEAS department and the Mission's CIS section to 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 personal or disciplinary data, or unauthorised use of data-processing systems by means of data transmission facilities.

d. Authorised users of data-processing systems cannot access any personal or disciplinary data other than those to which their access rights permit. The possibility to check logs and that personal or disciplinary 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 personal or disciplinary data it cannot be read, copied or erased without authorisation.

e. Logs are records of which personal and disciplinary data have been communicated, at what times and to whom, and provide the possibility to check the related logs.

f. Processing of personal or disciplinary data will be 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 personal or disciplinary data after the expiry of the retention period, which ensure the protection of personal or disciplinary 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 EEAS Data Protection Officer at data-protection@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.

Concerning to the data processed by the EEAS you have at any time the right of recourse to the European Data Protection Supervisor at edps@edps.europa.eu after your question has been treated by the EEAS Data Protection Officer at data.protection@eeas.europa.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 European Commission's Service for Foreign Policy Instruments (FPI) and the EUAM Iraq mission.