European Union Advisory Mission in Iraq

PRIVACY STATEMENT

regarding the processing and protection of personal data

related to closed-circuit television (CCTV) video surveillance in the Mission's premises and vehicles

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), the European Commission's Service for Foreign Policy Instruments of the European Commission (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 main purpose of the data processing activities (CCTV video surveillance system) is to ensure the protection of the Mission's security interests by deterring and preventing unauthorised access and entry to EUAM Iraq's premises, and to ensure duty of care, most importantly the safety and security of personnel and visitors but also including the Mission's premises, physical assets and information and reputation from harm and damage. CCTV includes cameras (dashcams) installed in the Mission's vehicles. Dashcams record video footage only, i.e. not audio.

The live stream from EUAM Iraq's CCTV cameras is monitored either by the Mission's Security and Health Department (SHD) staff or by staff members of the Mission's contracted security provider (GardaWorld).

The live stream footage is recorded. The recorded information is protected and safeguarded adequately.

Access to the recorded CCTV footage is only available for defined EUAM Iraq SHD personnel. For third parties external to the Mission, access is only authorised in duly justified cases and as set out below under Section 5.

The data may be used in case of disciplinary or criminal proceedings or to fulfil other legal requirements, including administrative instructions.

Your personal data will not be used for automated decision-making, including profiling.

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. Motion pictures of video footage recordings, raw or edited, and still images of persons and vehicles if registration plates or other means of identification, e.g. windshield signs, are visible.

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 (HOM), which in this capacity executes his or her duty as Data Controller. The Mission entity responsible for managing the visitor access control and the relevant database is the SHD under the supervision of the HOM.

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

The recipients of your data as recorded in live video or still pictures may include the following:

I. Within the Mission:
   a. HOM and all SHD personnel have access to all recorded footage.
   b. Personnel of the Mission's Communications and Information Services (CIS) personnel responsible for maintaining the Mission's CCTV system with single-event access authorisation from SHD staff, and by CIS personnel when acting as administrator of the Mission's network.
   c. Relevant persons involved in disciplinary proceedings, as applicable.

II. Outside of the Mission:
   a. Personnel of the Mission's contracted security provider only have access to personal data regarding those Mission premises and facilities they are responsible for. The personnel only have access to the current, daily record, not to historical data.
   b. Relevant Iraqi or EU or EU Member State public authorities involved in disciplinary or criminal proceedings or to fulfil other legal requirements, as applicable.
   c. 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 on grounds relating to your situation.

If you wish to exercise your rights or if you have any questions concerning the processing of your personal data, you may address them to the following functional mailbox: data.protection@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.

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, (CFSP) 2020/513 of 7 April 2020 and (CFSP) 2022/635 of 13 April 2022,
– Article 4.3.1.2 of the Mission's September 2026 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 be retained for thirty (30) days after the recording unless the recording will be needed for a legal or judicial procedure or for the purpose of audit and possible disciplinary or criminal investigation, in which case the personal data may be retained beyond the 30-day retention period, and for as long as it is necessary to complete the process.
2. In case of a complaint submitted to the European Ombudsman or 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, personal data may be retained for five (5) years after the closure of the case unless deletion occurred before the Mission received official request of retention after the normal 30-day retention period and the data thus was deleted.

II. Security of data:

1. Appropriate organisational and technical measures are ensured as follows:

a. In its electronic format, personal data will be stored in a EUAM Iraq database, which is a part of the Mission's CIS structure.
b. The stored, electronic files adhere to relevant, applicable security measures and by the confidentiality obligations deriving from the GDPR. The collected personal data will be processed by assigned mission members. Access to the files of the database is only granted to recipients with authorised, password protected administrative or viewer rights on a legitimate need-to-know basis and solely for the purposes of the processing operation, and only upon instruction of the Data Controller and only for the personal data that corresponds to their access rights.
c. Measures are provided to prevent non-responsible entities from unauthorised access, reading, copying, alteration, deletion or erasure, and/or removal or disclosure of personal data.
d. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.
e. Security is also ensured by the safety measures built into the various IT applications used.

9. Data protection contact: Do you have any questions regarding this statement?

If you have questions related to 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, the FPI and the Mission.