



EUROPEAN UNION MONITORING MISSION IN GEORGIA PRIVACY STATEMENT

FOR THE PURPOSE OF
PROCESSING PERSONAL DATA RELATED TO

Mission Visitor Access and registration of Visitors in the European Union Monitoring Mission in Georgia

1. INTRODUCTION

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

All data of personal nature - data that can identify you directly or indirectly - is handled with the necessary care.

2. PURPOSE OF THE PROCESSING: Why we process your data?

The main purpose of the data processing activity (register and control visitors' access to the premises of the Mission) is to ensure the protection of the Mission's security interests, Duty of Care, most importantly the safety of staff and visitors but also including Mission premises, physical assets, information and reputation from harm or damage.

3. DATA PROCESSED: what data we process?

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

I. Personal Data of Visitor

- First name and Last name
- ID-number (taken from the valid ID-document presented upon entry)
- Company or organisation
- Vehicle details
- Time of entrance and exit

II. Personal Data of the EUMM Georgia staff member receiving the visit

- First name and Last name
- Mission ID

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

Data Controller:

European Union Monitoring Mission in Georgia
Represented by the Head of Mission, Erik Høeg

5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?

The recipients of the data are the following, on a strict "need-to-know policy" basis:

1. Contracted Guard Company (Victoria Security) personnel, Contract Number: EuropeAid/139479/DH/SER/GE;
- Terms of Reference, Chapter 6. Requirements, paragraph 6.1. Staff, Scope of responsibilities for Expert 3: Security Guard, EUMM premises
2. Head of Mission
3. Deputy Head of Mission
4. Senior Mission Security Officer
5. Deputy Senior Mission Security Officer

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

You have the right to access your personal data and the right to request for correction of any inaccurate or incomplete personal data, as well as to request the removal of your personal data, if collected unlawfully, which will be implemented within 10 working days after your request has been deemed legitimate. If you have any questions concerning the processing of your personal data, you may address them to the following functional mailbox of the respective Data Controller:

contact@eumm.eu

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

- Council Decision: COUNCIL JOINT ACTION 2008/796/CFSP and its subsequent amendments, latest being COUNCIL DECISION (CFSP) 2016/2238
- OPLAN EEAS (2018) 1069 rev 1
- Civilian Operations Commander Instruction 12/2018 on the SOP on Personal Data Protection
- Security Handbook, January 2019
- STANDARD OPERATING PROCEDURES (SOP) ON SECURITY OF BUILDINGS AND ACCOMMODATIONS (02)

The processing is needed for the execution of the Mission mandate and HoMs' duty of care for security.

8. TIME LIMIT - DATA STORING: For what period and how we process your data?

Personal data shall not be kept longer than necessary. The documents or IT systems containing personal data, in hard copy or electronic format such as an ERP system, e-mail system and filing system will be retained during the following periods:

- Visitors' registry shall be retained for two years at the Mission and shall be available for audits or inspections.
- Photocopies of Identification documents are not stored

Visitors' badges do not contain personal data and may be recycled/reused without any limitations

Security of data:

Appropriate organisational and technical measures are ensured:

- In its electronic format the data will be stored in a server located within the Mission. The collected personal data are processed by assigned staff members. Files have authorised access. The database is accessible only to the recipients with the authorised administrative or viewer rights.
- Security is also ensured by the safety measures built in the various IT applications used.
- Measures are provided by CIS section to prevent non-responsible entities from access, alteration, deletion, disclosure of data.

Physical Files: Physical copies of the collected personal data will be stored in a properly secured and locked storage container.

The Mission has a system for the destruction of documents after the retention period expired. The system ensures the protection of the information contained in the document by permanent destruction, such as shredding, burning or deletion of back-up files in case of electronic data storage.

Administrative measures:

1. Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs;
2. Access to the data is limited to authorised personnel and it is subject to a password. Only a limited number of

employees can export the data – namely only international staff from the Security and Duty of Care Department.

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

In case you have questions related to the protection of your personal data, you can also contact the Mission Data Protection Advisor (MDPA) EUMM Legad, at the functional mailbox of the Mission contact@eumm.eu

10. RECOURSE

You have at any time the right of recourse that you may send to the Head of the Mission of EUMM, with the MDPA in copy.