EUPOL COPPS Privacy Statement

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO VEHICLE TRACKING SYSTEM BY THE EU MISSION FOR THE SUPPORT OF PALESTINIAN POLICE AND RULE OF LAW (EUPOL COPPS)

1. INTRODUCTION

THE PROTECTION OF YOUR PRIVACY INCLUDING YOUR PERSONAL DATA IS OF GREAT IMPORTANCE TO THE EUROPEAN UNION AND TO CSDP MISSIONS. WHEN PROCESSING PERSONAL DATA WE REFLECT THE PROVISIONS OF THE CHARTER ON FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, AND IN PARTICULAR ITS ART. 8. THIS PRIVACY STATEMENT DESCRIBES HOW THE CSDP MISSION PROCESSES YOUR PERSONAL DATA FOR THE PURPOSE IT HAS BEEN COLLECTED AND WHAT RIGHTS YOU HAVE AS A DATA SUBJECT. YOUR PERSONAL DATA ARE PROCESSED IN ACCORDANCE WITH THE PRINCIPLES AND PROVISIONS LAID DOWN IN THE PERTINENT LEGISLATION ON DATA PROTECTION, INCLUDING THE REGULATION (EC) 45/2001 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA BY THE COMMUNITY INSTITUTIONS AND BODIES AND ON THE FREE MOVEMENT OF SUCH DATA AND ITS SUCCESSIVE LEGISLATIVE ACT. ALL DATA OF A PERSONAL NATURE - NAMELY DATA THAT CAN IDENTIFY YOU DIRECTLY OR INDIRECTLY - WILL BE HANDLED FAIRLY AND LAWFULLY WITH THE NECESSARY CARE.

2. PURPOSE OF THE PROCESSING OPERATION

The purpose of the Vehicle Tracking System (VTS) is to ensure the Mission's duty of care over its personnel and ensure the rapid response in case of emergencies. The VTS also aims to ensure that the Mission can locate it's vehicles at all times.

3. DATA PROCESSED

The personal data covers the movement of personnel and Mission's Vehicles:

- Movement of personnel.

Appropriate organisational and technical security measures will be ensured according to the data protection legislation applicable to EU institutions and bodies.

Outline of Security Measures

Based on assessing risks related to potential access to data with regard to the process, the Mission ensures that adequate organisational and technical measures are in place in order to safeguard personal data of data subjects.

In order to protect the security of the data collected using VTS, including personal data, a number of technical and organisational measures have been put in place. These are detailed in a processing-specific security policy.

Among others, the following measures are taken:
I. Technical Measures

- Secure premises, protected by physical security measures, host the servers storing the images recorded; network firewalls protect the logic perimeter of the IT infrastructure; and the main computer systems holding the data are security hardened;
- The data is stored in local server in EUPOL COPPS premises.

II. Administrative measures

- Administrative measures include the obligation of all international EUPOL COPPS personnel having access to the system (including those maintaining the equipment and the systems) to have security clearance. Local staff can access the VTS system only when authorised by an international staff member.
- The employees of external security company have to sign a confidentiality agreement.
- Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
- Access to the data is limited to authorised personnel and it is subject to a password with personalised rights. Only a limited number of employees can export the data.
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to the criteria established in the Security Policy for Video-surveillance.
- The SOPs regulating the VTS contain an up-to-date list of all persons having access to the system at all times and

describes their access rights in detail.

4. CONTROLLER OF THE PROCESSING OPERATION

The Controller determining the purpose and the means of the processing operation is EUPOL COPPS. Mission's Security and Duty of Care is responsible for managing the personal data processing operation which is under the supervision of the *Acting Head of Mission Katja Dominik*.

5. RECIPIENTS OF THE DATA

VTS can be viewed "live" on a need to know basis, by:

- Mission officials, who need access to the footage for the performance of their duties. These are Mission security systems operators and their line of hierarchy in case of traffic or other security incidents.
- Mission internal investigators, appointed by and acting on instructions of the relevant Mission authority in disciplinary or security matters above;
- In exceptional circumstances and provided that there are adequate data protecion dafeguards in place, security and police authorities from the host country when the data collected using VTS concerns citizens from the host country or when granting such access is essential for mission security interests. The access can be granted only in duly justified circumstances, upon authorisation by the relevant Mission authority.
- Contractors of external companies in charge of Mission security and surveillance who, for the performance of their duties, need access to the VTS (subject to their 'need-to-know' and provided that they signed the confidentiality agreement).
- Others investigating EU, host country or other authorities, after approval of Security Authority, when appropriate.

Recorded data of the VTS can be processed by:

- The relevant Mission / EEAS authority in security matters.
- Mission / EEAS internal investigators, appointed by and acting on instructions of the relevant Mission /EEAS authority in disciplinary or security matters.
- In exceptional circumstances and provided that there are adequate data protecion dafeguards in place, security and police authorities from the host country when the data collected using VTS concerns citizens from the host country or when granting such access is essential for mission security interests. The access can be granted only in duly justified circumstances, upon authorisation by the relevant EEAS authority.
- Others investigating EU host country or other authorities after approval of the relevant EEAS authority in security matters, when appropriate.
- Initial data protection training is to be provided to all personnel with such access rights, including external subcontracted security guards. In particular, EEAS investigators receive instructions on personal data protection in the context of security investigations and sign a confidentiality undertaking.

External subcontractors and their personnel sign a confidentiality undertaking.

The information in question will not be communicated to third parties, except where necessary for the purposes outlined above

6. PROVISION, ACCESS AND RECTIFICATION OF THE DATA

You have the right to access your personal data and the right to correct 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 will have been deemed legitimate. If you have any queries concerning the processing of your personal data, you may address them to the functional mailbox: data-protection@eupolcopps.eu

7. LEGAL BASIS FOR THE PROCESSING OPERATION

Legal basis:

- Council Joint Action 2005/797/CFSP of 14 November 2005 on the European Union Police Mission for the Palestinian Territories as amended by Council Decision 2013/354/CFSP.
- SOP on Vehicle Tracking System (SEC/11).
- SOP on Transport/Use of Mission's Vehicles (TPT/001).
- Field Security Handbook for the protection of personnel, assets, resources and information of civilian CSDP missions.
- Guidelines for Vehicle Management.
- Civilian Operations Commander Instruction 12/2018 on the SOP on Personal Data Processing.
- SOP on Personal Data Protection (SOP/02).

8. TIME LIMIT FOR STORING DATA

Data will be retained for a time period determined in SOP on VTS and SOP on Transport/Use of Mission's Vehicles.

Information collected while using the VTS will be retained for the period of 7 years from the day it is collected. In case a traffic or other security incident occurs, the relevant data may be retained beyond the normal retention periods for as long as it is necessary to further investigate the security incident. The data may be retained for longer period also in cases the collected data is needed as evidence in disciplinary, administrative cases or court litigation.

The system is also monitored live by the security guards at the relevant reception areas 24 hours a day.

In case a traffic or other security incident occurs, the relevant data may be retained beyond the normal retention periods for as long as it is necessary to further investigate the security incident. The data may be retained for longer period also in cases the collected data is needed as evidence in disciplinary, administrative cases or court litigation.

9. DATA PROTECTION CONTACT: MISSION DATA PROTECTION ADVISOR

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

10. RECOURSE

You have at any time the right of recourse that you may send to the Head of the Mission within EUPOL COPPS, with the MDPA (Legal Advisor) in copy.