European Union
EXTERNAL ACTION

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE
FOR THE PURPOSE OF
PROCESSING PERSONAL DATA RELATED TO
THE USE OF VIDEO-SURVEILLANCE SYSTEMS IN THE EEAS

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS). You have the right under EU law to be informed when your personal data is processed as well as about the purpose and details of that processing.

When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular Article 8 on data protection. Your personal data are processed in accordance with Regulation (EU) 2018/1725 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 Regulation (EU) 2016/679, the General Data Protection Regulation.

In this privacy statement you find information about how the EEAS and EU Delegations process your personal data and what rights you have as a data subject.

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

Purpose

The purpose of this processing operation is to ensure the protection of EEAS security interests (including staff under the responsibility of the EEAS, EEAS premises, physical assets, information and visitors) as well as the safety of staff and visitors, by covering entry and exit points, pre-defined garage areas, rooms and corridors. When necessary, it complements other physical security systems such as access control systems and Intrusion Detection Systems.

The information recorded is protected and safeguarded in accordance with the EEAS Policy on video-surveillance systems is in line with the EDPS Video-surveillance Guidelines.

Description

The EEAS videosurveillance security system is based on surveillance cameras. The footage from the cameras is watched live by the external security company or by the EEAS Security Division in case of need. Access is granted to recorded images only by assigned EEAS staff members and are not available for the contracted security service provider.

Certain cameras, in a limited quantity, can be positioned and have a zoom.
At present, the EEAS has not installed covert comeras.
The EEAS may use covert cameras in exceptional circumstances for reasons of security and when decided by the Security Authority after notifying the DPO.

3. DATA PROCESSED: What data do we process?

The personal data concerned are video recorded images:

- Video sequences, live video image, i.e. real time footage
- Digital image recordings, i.e. recorded footage

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

The data controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Division responsible for managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

EEAS HQ Security and Security Policy, EEAS.BA.SI.2

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

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

- The relevant authority in security matters (including Head of BA.SI.2 Division and line of hierarchy);
- EEAS officials, who need access to the footage for the performance of their duties. These are EEAS security systems operators and their line of hierarchy;
- EEAS internal investigators, appointed by and acting on instructions of the relevant EEAS authority in security matters above;
- Security and police authorities from the host country, or, in exceptional circumstances, authorities from a third country when the footage concerns citizens from the specific third country or when granting such access is essential for EEAS security interests, in duly justified circumstances, upon authorisation by the relevant EEAS authority in security matters
- Contractors of external companies in charge of EEAS security and surveillance who, for the performance of their duties, need access to this footage (subject to their 'need-to-know');
- Other investigating EU authorities, including OLAF and IDOC, after approval of the EEAS Security Authority, when appropriate.

In case of recorded footage, images can be watched by:

- The relevant EEAS authority in security matters (including Head of BA.SI.2 Division and line of hierarchy);
- EEAS internal investigators, appointed by and acting on instructions of the relevant EEAS authority in security matters above;
- Security and police authorities from the host country, or, in exceptional circumstances, authorities from a third country when the footage concerns citizens from the specific third country or when granting such access is essential for EEAS security interests, in duly justified circumstances, upon authorisation by the relevant EEAS authority in security matters above;
- Other investigating EU authorities, including OLAF and IDOC, after approval of the 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 declaration.

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

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

You have the right of access to your personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed, taking into account the purpose of the processing. Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. For more detailed legal references, you can find information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. If you would like to exercise your rights or have questions concerning the processing of your personal data, you may address them to the Data Controller via the functional mailbox:

EEAS-SECURITY-POLICY@eeas.europa.eu
EEAS-SECURITY-ACCREDITATION@eeas.europa.eu
eeas-hq-security-coordination@eeas.europa.eu

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

Legal basis:

- Decision HR(2017) 10 of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service
- Decision HR(2013) 022 of the EEAS Chief Operating Officer of 7 November 2013 on the policy on video-surveillance systems

Further legal reference:
Good administrative practices in the framework of the Treaty of Lisbon and the Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) available on: http://www.eeas.europa.eu/background/docs/eeas_decision_en.pdf

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

Data will be retained for a time period determined in the EEAS Policy on video-surveillance systems, Data will be deleted at the end of the period outlined in the policy available upon request at entry to the EEAS.

The system is also monitored live by the security guards at the relevant reception areas 24 hours a day.
If a security incident occurs, the relevant footage may be retained beyond the normal retention periods for as long as it is necessary to further investigate the security incident.

Security of data

Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725. The collected personal data are stored on servers that abide by pertinent security rules. Data is processed by assigned staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/Password. Physical copies of personal data are stored in a properly secured manner.

In order to protect the security of the video surveillance system, including personal data, a number of technical and organisational measures have been put in place, which are detailed in the aforementioned processing-specific security policy.
The EEAS' security policy for video surveillance was established in accordance with Section 9 of the EDPS Video-surveillance Guidelines.

Among others, the following measures are taken:
I. Technical Measures
- Physical security measures protect the servers storing the recorded images.
- The recorded image sequences are stored on secured premises.

II. Administrative measures
- Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared.
- Access rights to users are granted to only those resources, which are strictly necessary to carry out the assignments.
- Access to the data is limited to authorised personnel and it is subject to a password with personalised rights. Only a limited mumber 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 Security Policy for Video-surveillance contains an up-to-date list of all persons having access to the system at all times and describes their access rights in detail.

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

If you have enquiries, you can also contact the EEAS Data Protection Officer at data-protection@eeas.europa.eu.

10. RECOURSE

You have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.