**EEAS Personal Data Processing Record**

Ref. Article 31 of Regulation (EU) 2018/1725 - Legal obligation for maintaining records

<table>
<thead>
<tr>
<th></th>
<th>Title of the processing activity</th>
<th>PROCESSING PERSONAL DATA RELATED TO THE USE OF VIDEO-SURVEILLANCE SYSTEMS IN THE EEAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Update of the record (last modification date)</td>
<td>10/12/2020</td>
</tr>
<tr>
<td>3</td>
<td>Register reference number</td>
<td>521</td>
</tr>
<tr>
<td>4</td>
<td>Identity and contact details of the Data Controller</td>
<td>Controller: European External Action Service (EEAS)   Directorate/Division responsible for managing the personal data processing activity: EEAS HQ Security and Security Policy, EEAS.BA.SI.2 R.P. Schuman 9/A, Brussels, 1040 Belgium  Contact Point: <a href="mailto:EEAS-SECURITY-POLICY@eeas.europa.eu">EEAS-SECURITY-POLICY@eeas.europa.eu</a>  <a href="mailto:eeas-hq-security-coordination@eeas.europa.eu">eeas-hq-security-coordination@eeas.europa.eu</a>  Processor:  External service provider in charge of EEAS security and videosurveillance Data Protection Officer:  Emese Savoia-Keleti, SG.AFFGEN.DPO  <a href="mailto:DATA-PROTECTION@EEAS.EUROPA.EU">DATA-PROTECTION@EEAS.EUROPA.EU</a></td>
</tr>
<tr>
<td>5</td>
<td>Identity and contact details of the Data Protection Officer</td>
<td>EEAS Data Protection Officer (DPO):  Emese Savoia-Keleti.  SG.AFFGEN.DPO  Functional Mailbox of the DPO:  <a href="mailto:DATA-PROTECTION@eeas.europa.eu">DATA-PROTECTION@eeas.europa.eu</a></td>
</tr>
<tr>
<td>6</td>
<td>Purpose of the processing activity</td>
<td>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 camaras.  The EEAS may use covert cameras in exceptional circumstances for reasons of security and when decided by the Security Authority after notifying the DPO.</td>
</tr>
</tbody>
</table>

Page: 1 of 4
### Categories of individuals whose data is processed - Data subjects

The surveillance system covers all individuals accessing the building of the EEAS or passing by in its immediate vicinity. In certain cases, to a limited extent, the surroundings of the buildings are recorded by the surveillance cameras, thus the images could cover third persons as well.

### Categories of data - Data processed

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

### Recipients of data – Access to 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.

### Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)

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.

### Time limit for keeping the data - Retention period

Data will be retained for a limited period of time 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.

### Data Storage

The video surveillance recorded image sequences are stored on hard disks via dedicated IT systems. Recorded images may be exported only for the purposes of an inquiry, including security investigations.

### General description of security measures

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. These are detailed in a 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

- 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 recorded image sequences are stored in special locked cupboards. These cupboards are located in the technical rooms with controlled access.

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 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.
- The exported data may be subject to an authentication control.

(Watermark)

- 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 (see Attachment 7); and
- 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.
| 15 | Rights of individuals | Data subjects have the right of access to their personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed, recorded images are only kept for a short period of time and cannot be modified. Under certain conditions, data subjects have the right to ask the deletion of their personal data or restrict their use as well as to object at any time to the processing of their personal data on grounds relating to their particular situation. The EEAS will consider data subjects’ request, take a decision and communicate it to the data subjects 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, it is communicated to data subjects that information can be found 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 data subjects would like to exercise their rights or have questions concerning the processing of personal data, they may address them to the Data Controller via the functional mailbox:   EEAS-SECURITY-POLICY@eeas.europa.eu   eeas-hq-security-coordination@eeas.europa.eu |
| 16 | Information to data subjects | Warning is displayed in the areas under surveillance with pictograms. The Privacy Statement linked to this Record contains the information provided to the Data Subject(s). The aforementioned distinct Privacy Statement is available on the intranet: https://eeas.europa.eu/sites/eeas/files/eeas_privacy_statement_videosurveillance_cctv_2019_update.pdf |