VIDEO-SURVEILLANCE POLICY

1. Introduction

The European Union Intellectual Property Office (EUIPO) operates a video-surveillance system (VSS), in the form of an integrated closed-circuit television (CCTV) system. The VSS is intended to ensure the safety and security of EUIPO buildings, assets, staff and visitors, and safeguard physical, informational and environmental security at the EUIPO by preventing unauthorised physical access to premises, damage to property and interference with information and information-processing facilities.

The video-surveillance policy ('this Policy') describes how this system is designed and operated, and details the safeguards in place to minimise its impact on personal data, privacy and other fundamental rights and legitimate interests of individuals affected by the VSS.

2. Objective

The objective of this Policy is to describe the VSS and the safeguards put in place by the EUIPO to ensure the protection of personal data, privacy and other fundamental rights and legitimate interests of individuals affected by the VSS. This Policy also sets internal procedures to ensure the VSS is in continuous compliance with the applicable legal framework.

The decision to use the VSS and adopt the safeguards described in this Policy was made by the EUIPO's Executive Director after due consultation with the Head of the Security Unit, the Data Protection Officer (DPO) and the Staff Committee, following internal procedures.

The EUIPO processes the images 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. In addition, this Policy follows the recommendations of the European Data Protection Supervisor (EDPS) video surveillance guidelines[1].

This Policy takes into account the SEAT Agreement signed between the EUIPO and the Kingdom of Spain (attachment 3). This agreement, which entered into force in 2012, provides for cooperation and coordination between the EUIPO and Spanish authorities on security matters. In addition, the Spanish Data Protection Agency was duly consulted in 2011.

2.1 Revision of the VSS

[1] EDPS video surveillance Guidelines: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

The EUIPO already operated a VSS before the EDPS guidelines on video surveillance were published in 2010. In 2011, where applicable, the EUIPO's procedures and safeguards on video surveillance were brought into line with the abovementioned guidelines and applicable legislation. This Policy updates the 2011 Security Policy for Video Surveillance.

2.2 Self-audit, ISO 27001, consultation and decision taking

The VSS was subject to a self-audit in 2012 and a data protection impact assessment in 2018 (attachments 1 and 2, respectively). Once a year, the system is audited within the framework of ISO 27001.

2.3 Transparency and periodic review

This Policy is prepared in two versions: a limited version and a publicly-available version on the EUIPO website: *https://euipo.europa.eu/ohimportal/en/euipo-video-surveillance-policy*

The publicly-available version does not include attachments, instead providing a summary of their contents due to the absolutely necessity of preserving confidentiality for security reasons.

This Policy will be subject to a periodic data protection review by the Security Unit every two years, with the first review being carried out by the end of 2020. During the periodic reviews the EUIPO will examine the need to maintain the VSS, whether it continues to serve its defined purpose, its scope and the existing alternatives. The review will take into account legislative developments to ensure this Policy continues to comply with the applicable legislative framework and with EDPS guidelines and recommendations. Copies of the periodic reports will also be attached to this Policy and available on the EUIPO intranet and/or website.

3. Areas under surveillance

The VSS comprises 269 cameras at the moment of publication of this Policy. A map showing their locations and a list of the cameras and their functionality are included in attachments 4 and 6. Cameras are located on the EUIPO premises, including its headquarters and other premises located abroad. Cameras monitor and/or record the external perimeter, all main building entrances, external emergency exits, secondary entrances, entrances to the car parks, access points through speed gates and revolving doors, restricted areas and highly restricted areas such as data centres.
All premises storing critical data, confidential information and computing critical equipment are classified as restricted areas[1] or highly restricted areas[2]. Restricted and highly

[1] 'Restricted areas' are areas such as the mailroom, archives, Design department and Central Security Control that can be equipped with basic physical security measures such as access control and with CCTV (no live/real-time monitoring).
[2] 'Highly restricted areas' are particularly vulnerable or vital areas such as the main and back up computer data centres, high-value storage areas, and essential/core service utility rooms which should be equipped with specific physical security

restricted areas are protected by specific security measures and controls to prevent unauthorised access. Access to these areas is granted only to authorised personnel for specific purposes. The list of EUIPO authorised personnel is attached to this Policy.

The cameras installed in the restricted areas will monitor only the entrances to these areas outside of work hours. The cameras will not be used for live (real-time) monitoring. Access is permitted only to the footage in case of physical security or electronic incidents.

The cameras in the highly restricted areas can be used for live monitoring (real-time monitoring).

Cameras do not monitor any areas subject to heightened expectations of privacy such as individual offices (including offices shared by two or more people and large, open-plan offices with cubicles), leisure areas, canteens, cafeterias, bars, kitchenettes, lunchrooms, lounge areas, waiting rooms, toilet facilities, shower rooms and changing rooms.

The above will apply in all instances except in the area that provides access to the Executive Director's office, where fixed-dome cameras are placed. These cameras are justified by the heightened security requirements, in particular concerning the safety and security of the Executive Director, his office and visitors, and the protection of highly sensitive and confidential information. This specific monitoring area is defined under the Physical Security Policy and reflected in the EUIPO Strategic Plan 2020 (attachment 5). Additional safeguards have been put in place in order to minimise the impact of this exception on the privacy of the persons concerned or potentially concerned. The cameras will not be used for live monitoring, but only for recording images. The records can be only accessed in case of an incident. Access to the records is password-protected and restricted to individuals holding specific credentials. Recordings by these cameras are encrypted. Adequate signage is required at entry points to the area, informing that it is under recorded video surveillance.

The location, and whenever needed, the masking function of all cameras, is carefully scrutinised in order to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes.

This is achieved by the following.

- Aligning video-surveillance monitoring and camera positions with the classification of building spaces and their security level as established in the Physical Security Policy.
- Directing fixed cameras to cover entrances and emergency access points in such a way that the coverage range is limited to the minimum necessary.
- Using the masking function of the cameras in areas subject to heightened expectations of privacy.
- Limiting the monitoring at the perimeter of the EUIPO premises in Spanish territory to an absolute minimum. Any change to the range and angle of cameras on the perimeter will be addressed under the SEAT Agreement.
- Using the masking function of the cameras to reduce coverage angles and exclude areas that should not be under surveillance, in particular along the perimeter.

---

measures (such as additional CCTV and biometric access control) in addition to the basic physical security measures applicable to restricted areas.

- Limiting zoom capabilities of cameras covering public spaces.
- Whenever possible, limiting monitoring to times when there are increased security requirements.
- Ensuring all security personnel have received adequate training on the VSS to guarantee the privacy of passers-by or others caught on the cameras is not disproportionately intruded upon.

4. Type of personal data collected

The VSS collects images of:

- data subjects entering/leaving/walking in public areas of the EUIPO premises and passers-by on the sidewalk adjacent to the exterior part of the perimeter fence;
- cars outside the premises when traversing car park and docks areas, and car park ramps, and cars passing on the street adjacent to the exterior part of the perimeter fence;
- data subjects and cars inside the premises in parking areas hallways;
- data subjects in the area adjacent to the Executive Director's office;
- data subjects inside highly restricted areas and at the entrances of restricted areas.

The cameras record digital images indicating time, date and location.

The VSS does not record images of persons in areas subject to heightened expectations of privacy, except for those cases specifically mentioned in this Policy and in compliance with the additional safeguards detailed. The system does not collect any special category of data.

Changes to the personal data being collected or the area under recording or surveillance will be consulted in advance with the DPO and will be duly justified for purposes in line with the objective of this Policy.

5. Purposes of the VSS

The purposes of the VSS are as follows:

- Detecting, deterring and preventing all kind of attacks, unlawful entry or other incidents (e.g. theft of assets, vandalism, flood, fire) at the EUIPO headquarters and external premises.
- Detecting, deterring and preventing attacks or unlawful entry in the entrance and exit areas.
- Detecting, deterring and preventing unlawful entry to the main buildings via the parking areas.
- Detecting, deterring and preventing incidents in common areas such as halls and parking areas.
- Detecting, deterring and preventing intrusions into highly restricted areas and restricted areas.

- Investigating the facts following physical security incidents and securing evidence to prosecute the perpetrator(s). The VSS is not an investigative tool. In exceptional cases the images may be transferred to investigatory bodies as part of a formal disciplinary or criminal investigation.

The VSS will not be used for any other purpose. There will be no use of hidden cameras for ad-hoc investigations or covert surveillance activities. There will be no special video surveillance for high-level events or demonstrations. The VSS will not be used to monitor the work of employees or to monitor attendance.

The footage will be used for its original purpose and the VSS will not be installed or designed for use in internal investigations beyond physical security incidents or electronic incidents (for instance, theft of information stored on a PC). Only in exceptional circumstances may the images be transferred to investigatory bodies or enforcement authorities as part of a formal disciplinary or criminal investigation, following prior consultation with the DPO, for instance in the context of the SEAT Agreement. The conditions under which the footage can be used in investigations are specified in paragraph 10 of this Policy.

6. Description and technical specifications of the VSS

The VSS is an integrated CCTV system. The VSS comprises detection and observation cameras, specifically fixed detection/observation cameras, fixed observation cameras, and PTZ (pan-tilt-zoom) dome observation cameras. The cameras may be set up or configured differently depending on the area monitored. Detection cameras can be set up to trigger an alarm in case of an intrusion or incident. PTZ dome observation cameras do not have an alarm function but have variable range and viewing angles and can be controlled manually by security personnel in case of an incident.

Fixed detection/observation cameras with an alarm setting are placed on the outer perimeter along with PTZ dome observation cameras, to detect intruders. The detection cameras watch the fence line and a silent alarm (which does not generate sound only image) is triggered when an intruder or object is detected. The footage from fixed detection/observation cameras is displayed on the control room’s video wall. The PTZ dome observation camera closest to the incident is activated and redirected to the location of the incident. Its footage is then displayed on the control room’s video wall and security personnel can control the camera manually to locate and track the intruder or object.

Fixed observation cameras are installed inside the buildings at some entrances or emergency exits. These cameras can be set up to trigger an alarm at the emergency exits. PTZ dome observation cameras are installed in the parking areas. Fixed observation cameras are located in the area adjacent to the Executive Director’s office. These are used only for recording, and never for live monitoring.

The general specifications of the cameras are as follows:

Fixed detection/observation cameras:

- are visual — when the alarm is activated the camera image automatically switches on the control room video wall;
- are connected to the control room;
- cannot be manually controlled or redirected;
- cannot be zoomed in and out, or panned side to side;
- have image masking functions.

Fixed observation cameras:

- cannot be manually controlled or redirected;
- cannot be zoomed in and out, or panned side to side;
- can be triggered by an alarm and connected to the control room video wall.

PTZ dome observation cameras:

- are installed along the perimeter, on roofs, in the car park and at the entrance to the main hall;
- can zoom in and out, and also be panned side to side;
- have their images blurred or masked to avoid footage of external private buildings and parking areas;
- can be programmed by the external security company if so instructed by the EUIPO.

The VSS is monitored by security personnel who watch the footage in real time on the video wall of the control room, 24 hours a day and 7 days a week. The cameras recording the area providing access to the Executive Director's office are an exception from this.

The camera hardware inventory list is available in attachment 6. It specifies the cameras' brand, type, function (detection or observation) and hardware version.

All cameras mask private areas or areas subject to heightened expectations of privacy. PTZ dome observation cameras have additional safeguards in place to protect privacy, such as limits on their zoom and remote control capabilities.

7. Legal basis for video surveillance

The use of the VSS is necessary for the correct management and functioning of the EUIPO in line with the purposes stated above and in accordance with Article 5.1(a) and Article 5.1(e) of Regulation (EU) 2018/1725. In addition, it finds its legal instrument in Article 150 of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trade Mark (EUTMR), which requires the Office to apply the security principles contained in the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, as set out in Commission Decisions (EU, Euratom) 2015/443 and 2015/444.

8. Access to the VSS images

The images can only be accessed in two ways: via live monitoring or via access to stored footage. Access depends on the role of the person concerned. Access rights and credentials are granted to users on a need-to-know basis to carry out their tasks.

An up-to-date list of all persons who have been granted access to the VSS, with their names, functions and type of access, is provided in attachment 7. Access will be via a password-protected desktop computer in the control room, secured by the credentials granted to the specific user. Access to technical features such as copying, downloading, deleting or altering footage is provided following the rules stated in attachment 7 and following prior consultation with the DPO.

Each actor having access to the live monitoring and/or stored footage will sign a confidentiality statement. In addition, external security personnel will handle sensitive privacy information in accordance with personal confidentiality agreements. They can use the PTZ dome observation cameras' pan and zoom functions only in the case of an alarm and if there is a security-related reason to do so. In case of a security incident or doubt they will consult with the external security company coordinator, who, correspondingly, in case of need, will immediately consult the Security Officer, Security Seconded National Expert and Security Coordinator.

The security system's maintenance provider will neither monitor live footage nor have access to recorded footage, except with the authorisation of and under supervision by EUIPO staff, and then only for the time necessary to perform technical maintenance tasks related to the VSS. The security system's maintenance provider will act solely under the instructions of the EUIPO's Infrastructures and Buildings Department (IBD) Director and Security Officer and in order to secure the smooth and correct functioning of the VSS. The specifications annexed to the framework contract concluded with the security system's maintenance provider contains a confidentiality clause and ensures the implementation of technical and organisational security measures to comply with data protection requirements. The employees of the security system's maintenance provider sign a confidentiality agreement and are required to be in possession of an official certificate of good conduct. The provider is required to comply with the ISO 27001 standard. A description of EUIPO security environment data protection measures concerning the security system's maintenance provider is available in attachment 8. The contract with the provider is included in attachment 9.

9. Data protection training

Specific data protection training is an obligatory requirement for all personnel with access to live monitoring data or recorded data.

Training is provided for each new member of staff, and periodic workshops on data protection compliance issues are held at least once every two years for all staff with access rights.

External security company coordinators and on-duty external security personnel must hold an official security certificate issued by an academy approved by the Spanish Ministry of

Home Affairs and comply with the Spanish Law on Private Security 5/2014 and Regulation on Private Security. In addition, they must complete 20 hours per year of compulsory training, of which an adequate number of hours will be allocated exclusively to data protection training. These requirements will ensure up-to-date training in data protection.

10. Transfers and disclosures

No transfer or disclosure of data recorded by the VSS will be made except by written authorisation of the IBD Director, after consulting the DPO. All transfer or disclosure requests are subject to a thorough assessment as regards their necessity and the compatibility of their purpose with that originally pursued by this Policy. All transfers and disclosures are to be documented, registered and kept in electronic format. The template to be used is enclosed as attachment 10.

Images or footage may be transferred to investigatory bodies as part of a formal disciplinary or criminal investigation, involving entities such as:

- EU organisations such as the Anti-Fraud Office (OLAF) or the Investigation and Disciplinary Office of the Commission (IDOC), as part of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Union;
- Spanish law enforcement authorities, under the observance of the agreement regarding coordination on security matters set out in the SEAT Agreement signed between the EUIPO and the Kingdom of Spain;
- private entities such as insurance companies; following consultation with the DPO and upon approval of the ICLAD Director and IBD Director.

11. Data and information protection measures

In addition to the measures detailed above about access to data, and the specific safeguards envisaged to deal with the existing exception, the EUIPO will put in place a number of protective technical and organisational measures, as follows:

- Internal and external premises are to be protected by physical security measures.
- Servers where recorded images are stored are to have additional physical protection measures. Archives of stored footage are to be placed in restricted areas and access to digital records is to be password protected.
- Recorded and stored data is to be encrypted in order to mitigate the risk of unauthorised access.
- File(s) where recorded material is kept after an incident are to be password protected. The PC where these files are located is also to be password protected.
- A reliable digital logging system must be in place to ensure that an audit can determine at any time who accessed the VSS, where they accessed it from and when they accessed it. The logging system has to be able to identify who viewed, deleted, copied or altered any surveillance footage.
- The IT infrastructure’s logical network perimeter is to be protected by firewalls.
- The main computer systems holding the data are to be hardened with additional security measures.

- All outsourced personnel having access to the VSS (including those maintaining the equipment) are to be cleared by security.
- Cameras are to be protected by tamper switches and camera access is to be password protected. Cameras are to run under password protection.
- Software is to be password protected. Perimeter cabling redundancy is to be ensured using the chain principle.

12. Retention period

Camera footage will not be stored for more than 7 days. When this period expires, the data will be automatically deleted. In case of an incident, a backup of the corresponding video footage may be stored for the time necessary to investigate and solve the incident. This period can be extended until the resolution of a possible complaint or appeal. Any additional retention period is documented and registered, and its necessity is reviewed regularly. As soon as the purpose of the investigation and eventual complaint or appeal ends, the images will be deleted. The DPO is always informed of the extension of the retention period and the deletion of the footage when its purpose is fulfilled.

13. Public information and specific individual information

Information on the presence of the VSS will be made available to the public. This information will be provided by means of local signage and by the publication of this Policy.

- The signs are to be placed near the cameras and at the access points to the buildings (including the main entrance), parking areas and on the perimeter fencing. These signs are to inform the public of the presence of video-surveillance cameras and provide the following information:

    - the identity of the controller, (the EUIPO);
    - the purpose(s) of the surveillance (for safety and security);
    - an indication of whether the images are recorded;
    - contact information and a link to this Policy;
    - the retention period of the images.

If any area outside the buildings is under surveillance, this will be clearly stated.

The size of the signs (A2, A3 or A4) will vary depending on the type of camera used in the specific area. An example of the EUIPO's local data protection signage is included as attachment 11.

This Policy is available both on the EUIPO's website and on the home page of the EUIPO intranet (Insite).

In addition, EUIPO staff will be given individual notice if they were specifically identified in recorded or live monitoring footage (for example, by security staff as part of a security investigation) if one or more of the following conditions also apply:

- their identity is noted in any files or records;

- the video recording is used in a formal proceeding against the individual;
- the video recording is kept beyond the regular retention period;
- the video recording is transferred outside the Security Unit; or
- the identity of the individual is disclosed to anyone outside the Security Unit.

Notice may be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences. The DPO is consulted beforehand in such cases.

14. Rights of the data subject

Persons recorded by the VSS will have the right to access the footage, and the right to rectification, object, erasure and restriction of processing as described in QSD 0295 DPO and DPCs work instruction. For that purpose, a viewing of the images may be organised or a copy of the recorded footage may be provided free of charge. This copy will not reveal personal data of other data subjects. In order to ensure the protection of personal data of other data subjects and balance the interests of the requester with the rights of other data subjects, the DPO will be informed before any viewing or before any copy of recorded footage is handed over, and whenever possible will be present at the viewing or handover. In order to guarantee the respect of other data subjects' rights, additional technical measures are put in place, such as masking or blurring images of others before the viewing or handover. The requester needs to demonstrate legitimate interest, identify themself, motivate their request and state the data, time, location and circumstances in which they were filmed. The access request will be sent to the Security Unit, which will respond to the query in a diligent manner and within one month of the receipt of the request, to ensure the effectiveness of the requester's right of access. It will not be possible to accommodate requests made more than 7 days after the date of the original footage due to the 7-day retention practice.

The rights of data subjects may be restricted as described in QSD 0295 DPO and DPCs work instruction when this restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a) the national security, public security or defence of the Member States;
b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security: for instance, in case of an on-going investigation by law enforcement bodies;
c) other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
d) the internal security of Union institutions and bodies, including of their electronic communications networks;
e) the protection of judicial independence and judicial proceedings;
f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

g) the monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c);
h) the protection of the data subject or the rights and freedoms of others;
i) the enforcement of civil law claims: for instance, when recorded material may help to prove the enforcement of a civil claim.

15. Right of recourse

Individuals can address queries to the EUIPO's Director of the Infrastructures and Buildings Department, at the following email address: DPOexternalusers@euipo.europa.eu

You may consult the EUIPO Data Protection Officer at the following email address: DataProtectionOfficer@euipo.europa.eu.

If the request has not been responded to adequately by the data controller and/or DPO, data subjects can lodge a complaint with the European Data Protection Supervisor at the following email address: edps@edps.europa.eu."

Attachments to the Video-Surveillance Policy (Limited)

1. Self-audit in 2010
2. Privacy Data Protection Impact Assessment EUIPO Video-Surveillance
3. SEAT Agreement
4. Map with the locations of the cameras
5. EUIPO Strategic Plan 2020
6. Camera hardware list
7. List of access to the video surveillance system: functions and types of access
8. Provider's description of the EUIPO security environment data protection measures
9. Contract with Security Provider
10. Template for transfer and disclosures
11. On-the-spot data protection notice
12. List of the EUIPO restricted and highly restricted areas