



CPVO • OCVV

Community Plant Variety Office
Office Communautaire des Variétés Végétales

ON-LINE DATA PROTECTION NOTICE OF VIDEO SURVEILLANCE IN THE COMMUNITY PLANT VARIETY OFFICE

For your safety and security, the Agency operates a video-surveillance system. This notice

- Provides you with basic information about the system,
- Tells you where you can get more detailed information, and
- Explains how you can exercise your rights as a data subject.

1. What areas are under surveillance?

The video-surveillance system consists of a set of seven cameras. Of these, six cameras are located at the main building at the entry and exit points, including the main entrance, the lateral entrance, the entrance to the exterior parking, the entrance door at the underground parking and the gate (but no images are recorded from this last camera). In addition, there is also a camera at the entrance to the n° 9 building. There are no cameras located elsewhere either in the buildings or outside them.

2. What is the lawful ground and legal basis of the video-surveillance?

The use of our video-surveillance system is necessary for the management and functioning of our Agency. The use of video-surveillance system in the CPVO meets the requirements stated in the Regulation No 45/2001.

3. What personal information do we collect and for what purpose?

The video-surveillance system is a conventional static system equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. The image quality in most cases allows your identification (though it is not accurate) if you are in the camera's area of coverage. The cameras are fixed, and thus, cannot be used by the operators to zoom in on you or follow you around.

The Agency uses its video-surveillance system for the sole purpose of security and access control. The video-surveillance system helps control access to our building and helps ensure the security of the building, the safety of our staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access cards and code access and night alarms. It forms part of the measures taken pursuant to our broader security policies and helps prevent, deter, and if necessary, investigate unauthorized physical access, including unauthorized access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance

3, Bd. Maréchal Foch - BP 10121 - 49101 Angers Cedex 02 - France - Tel. +33 (0)2 41 25 64 00 - Fax +33 (0)2 41 25 64 10 - cpvo@cpvo.europa.eu - www.cpvo.europa.eu

Служба на Общността за сортовете растения • Oficina Comunitaria de Variedades Vegetales • Odrůdový úřad Společenství • EF-Sortsmyndigheden • Gemeinschaftliches Sortenamnt • Ühenduse Sordiamet • Κοινοτικό Γραφείο Φυτικών Ποικιλιών • Community Plant Variety Office • Office communautaire des variétés végétales • Ufficio comunitario delle varietà vegetali • Kopienas Augu šķirņu birojs • Bendrijos augalų veislių tarnyba • Közösségi Növényfajta-hivatal • L-Ufficju Komunitarju dwar il-Varjetajiet tal-Pjanti • Communautair Bureau voor plantenrassen • Wspólnotowy Urząd Ochrony Odmian • Instituto Comunitário das Variedades Vegetais • Oficiul Comunitar pentru Soiuri de Plante • Úrad Spoločenstva pre odrody rastlín • Úrad Skupnosti za rastlinske sorte • Yhteisön kasvilajikevirasto • Gemenskapens växtsortsmyndighet

helps prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff or threats to the safety of personnel working at the office (e.g. fire, physical assault).

The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. The system is also not used as an investigative tool or to obtain evidence in internal investigations or in disciplinary procedures, unless a security incident is involved. (In exceptional circumstances the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in section 4 below).

4. Who has access to your information and to whom is it disclosed?

Recorded video is accessible only to the responsible of the video-surveillance system. Live video is also accessible to the receptionist.

All transfers outside the CPVO are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing.

No access is given to management or to the human resources service.

Local police may be given access if this is needed to investigate or prosecute criminal offences.

Under exceptional circumstances, and subject to the procedural safe guards noted above, access may also be given to

- The European anti-Fraud Office ("OLAF") in the framework of an investigation carried out by OLAF,

provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or criminal offence.

5. How do we protect and safeguard your information?

In order to protect your personal data, a number of technical and organizational measures have been put in place. 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 system holding the data are security hardened. All staff signed non-disclosure and confidentiality agreements.

Access rights to users are granted only to the extent strictly necessary to carry out their jobs. Only the system administrator specially appointed by the controller for this purpose is able to grant, alter or annul any access rights of any person, after being instructed to do so by the President of the CPVO. Any grant, alteration or annulment of access rights is made pursuant to the criteria established in our security policy for video-surveillance, which forms an integral part of our video-surveillance policy.



6. How long do we keep your data?

The images are recorded for a maximum of 7 days. Thereafter, all images are deleted. If any images need to be stored for further investigation or evidence of a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed.

The system is also monitored live by the receptionist during her working hours.

7. How can you verify, modify or delete your information?

You have the right to access the personal data we hold regarding you and to correct and complete them. Any request for access, rectification, blocking and/or erasing of personal data should be directed to the President of the CPVO and consult it with the CPVO's Data protection officer (dpo@cpvo.europa.eu). He/She may also be contacted in case of any other questions relating to the present processing of personal data.

Whenever possible, the CPVO must respond to an enquiry in substance within 15 calendar days. If this is not possible, you will be informed of the next steps and reason for the delay within 15 days. Even in the most complex cases you will be granted access or a final reasoned response for the rejection of your request within three months at the latest. The CPVO will do its best to respond earlier, especially if you establish the urgency of the request.

If you specifically request so, a viewing of the images may be arranged or you may obtain a copy of the recorded images on a DVD or other customary support. In case of such request, please indicate your identity beyond doubt (e.g. you may bring identification cards when present yourself for the viewing) and also designate the date, time, location and circumstances when you were caught on cameras. Please also provide a recent photograph that allows the security staff to identify you from the images reviewed.

At this time, we do not charge you for requesting a viewing or a copy of your recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

Please note that we cannot always provide you with an image, as exemptions under article 20(1) of the Regulation (EC) n° 45/2001 apply in a specific case. For example, upon a case-by-case evaluation we may have to conclude that restricting your access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

8. What is our compliance status with applicable data protection laws?

The CPVO processes your images in accordance with the video-surveillance guidelines issued by the European Data Protection Supervisor and Regulation (EC) n° 45/2001 on the protection of personal data by the Community institutions and bodies.



The system was subject to a self-audit. Considering the limited scope of the system, it was not necessary to submit a prior checking notification to the EDPS but we notified him of our compliance status by sending him a copy of our video-surveillance policy and data protection compliance report. A periodic data protection review is undertaken by the CPVO every two years.

For further information please consult:

- http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-07-07_Consultation_videosurveillance_guidelines_EN.pdf;

9. Right to recourse

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EC) 45/2001 have been infringed as a result of the processing of your personal data by the Agency. Before you do so, we recommend that you first try to obtain recourse by contacting the CPVO's Data protection Officer (dpo@cpvo.europa.eu).

If you are a staff member you may also request a review from your appointing authority under Article 90 of the Staff Regulation.

