Privacy Statement on the processing of personal data in the context of the Video Surveillance System

1. Context and Controller

The personal information we collect from you ("the Data Subject") will be processed in line with Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals 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 ("Regulation (EU) No 2018/1725" or "EUDPR").

Your privacy is important to the Community Plant Variety Office ("CPVO" or "us" or "the controller") and we feel responsible for the personal data that we process on your behalf. Therefore, we are committed to respecting and protecting your personal data and ensuring the efficient exercising of your data subject's rights.

2. What personal data do we process and why?

The video system records digital images together with time, date and location. Unless there is a request to access to the recordings, no further processing is done until the data are overwritten with new records after a period of 30 days.

Real-time monitoring is possible through the monitors at the reception desk. These monitors do not provide access to recorded footage.

The purpose of using the video-surveillance is to ensure the safety and security of CPVO's buildings, assets, staff and visitors. The video-surveillance system reinforces access control and security of the buildings, the safety of the staff members and visitors, as well as the property and information located or stored on the premises.

3. What are the legal basis and the ground for lawfulness of processing?

The legal basis for the processing of data is Article 5.1 (a) of Regulation (EU) 2018/1725 ("the processing is necessary for the performance of a task carried out in the public interest").

4. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the IT Unit.

5. Who has access to your personal data and to whom is it disclosed?

The data may be disclosed to the following:

Within the CPVO:

The security guards monitor live-streaming images to control access to the buildings. The IT System Administrator (and his/her replacement within the IT Unit) may access the footage following previous authorisation of the President.

Outside the CPVO:

In case of security accidents or official inquiries, data may be disclosed to the European Commission Anti-Fraud Office (OLAF) and/or the national police.

6. How do we safeguard your personal data?

The controller implements appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to it.

As for the live-streaming, the location of the screen at the reception desk prevents any unauthorised viewing of the images from the camera.

As for the recordings, the video-surveillance system's hard drive is stored in a securely locked room. Access to the room is protected by password and a physical key. Access to the room is restricted to the IT System administrator and his replacement. Access to the hard-disc recorder (where the footage is located) is highly limited, being username and password protected, and recording any log or action from the staff members. The hard-disc recorder is not connected to internet.

The footage may be monitored only in case of a security accident or due to an access request from the data subject or a third party. However, data can be accessed only following previous authorization of the CPVO President (acting as controller) and access is restricted to the IT Systems Administrator. The IT Systems Administrator is responsible for investigating security accidents.

7. How long do we keep your data?

The images are recorded for a maximum of 30 days. The procedure of erasure is done automatically and periodically by overwriting the media support on a first-in and first-out basis.

8. How can you obtain access to information concerning you and, if necessary, rectify it? How can you request the erasure of your personal data or restriction of processing or object processing? How can you request to exercise your right to data portability? How can you withdraw consent, where processing of your personal data is based on consent?

If you would like to request to obtain access to information concerning you and, if you think that it is necessary, to correct it, to request the erasure or restriction of processing of your personal data and/or object to processing of it; if you would like to request to receive the personal data concerning you in a structured, commonly used and machine-readable format and to transmit those data to another controller, you may contact us. In exercising your right to data portability, you also have the right to have your personal data transmitted to another controller, where technically feasible.

Right to object: We are using your personal data because we believe that it is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority vested in the CPVO. In case you disagree with the processing of your personal data, based on the aforementioned lawful ground, you have the right to object, at any time.

Right to withdraw consent: You have the right to withdraw your consent at any time.

Right to access: You have the right to access and confirm what personal data we hold about you, at any time.

Right to rectification: You also have the right to correct inaccurate personal data.

Right to erasure: You have the right to "erase" your personal data.

Right to data portability: You have the right to receive your personal data, which we have collected from you based on your consent, from us and to transfer or have it transferred (where it is technically feasible) to another controller.

Right to restrict the processing: When certain conditions apply, you have the right to request that we restrict the processing activities relating to your personal data.

If you would like to exercise any of these rights, please send us your request. We will provide information on action taken on your request 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, taking into account the complexity and number of the requests. We shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

In case you wish to request access to your personal data, to verify which personal data we store on your behalf, have it modified, erased, restrict the processing, exercise your right to data portability, object or withdraw consent, please make use of the contact information mentioned, by explicitly and accurately describing your request.

In principle, we cannot accept verbal requests (telephone or face-to-face) as we may not be able to deal with your request immediately without first analysing it and reliably identifying you. Requests can be sent to the controller: Head of the Administrative Unit by e-mail at dpc@cpvo.europa.eu.

9. Who should you contact if you have a question about the protection of personal data or in case you would like to lodge a complaint?

Should you have any queries in relation to the processing of your personal data, please address these to the data Controller, at the following email address: dpc@cpvo.europa.eu.

You may also consult the CPVO's Data Protection Officer: dpo@cpvo.europa.eu.

Complaints, in cases where the conflict is not resolved by the controller and/or the Data Protection Officer, can be addressed at any time to the European Data Protection Supervisor: edps@edps.europa.eu.