CPVO
Community Plant Variety Office

DATA PROTECTION REGISTER

COMMUNITY PLANT VARIETY OFFICE (CPVO)

CPVO
Community Plant Variety Office

Disclaimer

This document contains the centralised Register of Records of the personal data processing activities of the Community Plant Variety Office (CPVO), as established in accordance with Article 31(5) of 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.

The records in the Data Protection Register of the CPVO contain the information required as per Article 31(1) of Regulation (EU) 2018/1725. To ensure that the information provided is accurate and up-to-date, the Register is being regularly reviewed and the records internally validated by the concerned CPVO Data Controllers.

For further information or for addressing any query concerning the CPVO register, please contact directly the CPVO Data Protection Officer (DPO) (dpo@cpvo.europa.eu) or the concerned Data Protection Coordinator (DPC) (dpc@cpvo.europa.eu).

This current version of the CPVO Data Protection Register contains the CPVO records of data processing operations as updated and accordingly internally validated by the concerned CPVO Data Controllers by ***15 April 2021***.

Index of Data Protection Records

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Deposit of IT Equipment for Home Use and Use of Pulse Secure

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 01

4. * Name and contact details of the Controller:

Head of IT Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

IT Unit and Legal, Procurement and Logistics service

7. Description of the processing operation:

An employee who wishes to use CPVO IT equipment at home must fill in a form. IT Unit shall allocate the equipment to the employee in question. Before the equipment is given to the employee, the IT Unit checks if it is operational and functioning well. The employee signs the form by which acknowledges he/she received the equipment. A register of equipment deposited and where it was deposited is kept by the IT Unit.

As for the use of Pulse Secure, this is a software that enables secure remote access from the employee's home equipment (both private and CPVO IT equipment) to the CPVO' servers. The software is installed in the home equipment by the IT Unit and the employee working from home is required to activate the VPN connection. This latter is the process by which a secure connection can be established between remote network devices, particularly between the VPN client (staff member's device) and server device (CPVO server). The VPN connection is only established when the client device authenticates itself on the VPN server.

The authentication method is twofold and cumulative, for security reasons. The Staff member is required to enter his username and password within the Pulse Secure window on the device used for teleworking and then proceed with the second authentication method by using the two-factor authentication (2FA) provided by the "RSA SecurID Token". This token is installed by the Staff member on a different device than the one used for teleworking (usually mobile device) and provides a unique code (every minute) to be typed in the Pulse Secure window on the device used for teleworking. The appliance system provided by Pulse Secure displays the relevant information of every VPN client, and it is accessed by the IT Administrator only with the purpose of debugging. The server of Pulse Secure is installed within the CPVO's premises. In phase of authentication, Pulse VPN communicates with the "RSA SecurdID" to validate the token entered.

The "RSA SecuID" server is located within the CPVO premises and only communicates with Pulse server to authenticate CPVO staff members.

8. * Purpose(s) of processing and legal basis:

In fulfilling their duties, employees of the Office sometimes work from home, purpose for which the Office allows the deposit of IT equipment, such as PCs and screens, at the employees' home. Furthermore, with the aim of ensuring secure remote connection, business continuity and services availability, data is collected and stored into the appliance system, so that the IT Unit can intervene in case of bugs related to the remote connection.

Legal instruments:

- Article 1e (3) and Article 20 of the Staff Regulations of Officials;
- Article 16 of the Conditions of Employment of Other Servants of the European Communities (CEOS);
- Decision of 11 December 2017 on implementation of telework in the CPVO;
- Decision of 31 March 2021 on telework from outside the place of employment.

Legal basis:

Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO staff members and trainees, who wish to use CPVO IT equipment at home as well as those who telework from home.

10. When and how were data subjects informed:

The Privacy Statement is available to CPVO staff members at the Intranet of the Office, Sharepoint, under the Data Protection Officer section. Data subjects are informed about where to find the Privacy statement before filling in the request for IT equipment. The decisions on the implementation of telework and telework outside the Office are also available to data subjects on the CPVO Intranet, Sharepoint.

When receiving the IT Equipment, data subjects are informed about the procedure to download and install "RSA SecurdID" on their mobile device.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data collected are:

- Name, surname or (sometimes) initials of the employee or trainee in question;
- Description and inventory number of the equipment (only for IT home equipment);
- Signatures of the staff member or trainee (only for IT home equipment);
- External IP address (only for Pulse Secure and RSA);
- Time of connection and disconnection (only for Pulse Secure and RSA);
- Name of the laptop used and operating system details (only for Pulse Secure and RSA).

The identification number of the equipment/serial number is located on the equipment itself.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Paper based documents containing personal data are store in the Office of the IT Administrator. In case of electronic copies (acceptance form and register of equipment deposited), data is stored in the internal database of the CPVO "Docman" and access is restricted to the IT Unit and the Procurement Service.

Data collected by Pulse Secure is stored into the appliance system of Pulse Secure. This latter is password protected and access is restricted to the IT Administrator within the IT Unit. In case the IT Administrator in charge of it is not present, access may be granted to a substitute within the same Unit.

Data collected by the token "RSA SecurID" is stored in the internal server of the CPVO.

14. The recipients or categories of recipients to whom the data might be disclosed:

As for the equipment for home use, data may be disclosed to the Head of Unit of the staff member, the responsible Financial assistant, the Procurement service within the Legal Service and the IT Unit on a *need-to-know* basis.

Data collected through Pulse Secure and available via the appliance system, is accessed only by the IT staff member within the IT Unit for debugging. If the staff member in charge of the use of Pulse Secure is not present, access may be granted to a substitute within the same Unit.

Data collected through "RSA SecurID" may be accessed only by the IT administrator or in case of absence, by his substitute within the IT Unit.

15. * Period of retention for the data:

As for the equipment for home use, data is retained until the equipment is returned by the staff member. Upon return of the equipment, electronic copies of the data processed are promptly deleted manually.

As for the use of Pulse Secure and RSA, data is stored within the appliance system of Pulse Secure for 6 months, after which data is manually deleted by the responsible person within the IT Unit.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

Regarding the IT equipment for home use, the physical file is kept in a locked cupboard. Electronic and scanned files are stored within CPVO' servers and accessible only by the IT Unit and the procurement service within the Legal Service based on the *need-to-know* principle.

As for the use of Pulse Secure, the appliance system where the personal information is stored and displayed is password protected and only accessible by the IT administrator within the IT Unit. In case the staff member in charge of it is not present, access may be granted to a substitute within the same Unit. Data is stored within the CPVO' servers.

As regards the use of the token "RSA SecurID", this authentication method is disconnected to the cloud and uses only the Authentication Manager, an internal server within the internal IT infrastructure of the CPVO. The server only communicates with Pulse Secure' server (internal) to further authenticate the users. The Server may be accessed only by the IT administrator for purposes of debugging.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Residence Permit

2. * Last update of this record:

19/03/2021

3. Reference Number:

No 2

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

Upon the employment of a new staff member (official, temporary or contract agent), the Human Resources (HR) sector of the CPVO collects the data mentioned below and fills in the "Fiche Individuelle" and "Notification de Nomination et de Prise de Fonctions" for obtaining the "attestation de fonctions" or the "titre de séjour special ID card", required by the French Ministry of Foreign Affairs.

The "attestation de fonctions ID" is required for French nationals, people with a dual nationality (French and foreign) and long-term residents (people of a foreign nationality who already lived in France before starting working for the CPVO). The "titre de séjour spécial ID card" is required for foreign nationals.

The applications are submitted by HR to the French Ministry of Foreign Affairs along with a cover letter and photos of the staff member. The Ministry retains these applications and provides the "titre de séjour special ID card" generally issued within 3 to 5 weeks after receiving the complete application.

The request for the special ID card is added to the personal file of the data subject. Once the HR sector receives the "titre de séjour special ID card", it makes a copy of the same and retains it in Docman (internal IT tool for electronic storage of documents), in the staff member's personal file.

Internally, the HR sector also maintains an Excel sheet to keep record of the expiry of the "titre de séjour special ID card" for the purpose of submitting to the French Ministry of Foreign Affairs another application namely "Changement de Situation du Titulaire" for renewal or prolongation of the validity of the cards.

For staff members with diplomatic status (President and Vice-President of the CPVO), the "attestation de fonctions" or "titre de séjour special ID card" provides, as appropriate, inviolability and immunity from jurisdiction, more or less extensive and limited in any case to acts performed in the exercise of functions, in accordance with the "Protocole sur les privilèges et immunités des Communautés Européennes".

The CPVO can also handle the process for obtaining the "titre de séjour special ID card" for the family members/relatives/spouse of a staff member upon his/her request. The same described process applies.

8. * Purpose(s) of the processing and legal basis:

The processing is necessary to provide CPVO staff with special French "attestation de fonctions" or "titre de séjour special ID card" to lawfully reside in France.

Legal Instrument:

Protocol No 7 on the Privileges and Immunities of the European Union.

Legal Basis:

Article 5.1 (a) of the Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

All staff employed by the CPVO (French and non-French nationals) employed for more than 6 months and, where applicable, their family members/relatives.

10. When and how were data subjects informed:

Data subjects are informed via e-mail by the HR sector about the "attestation de fonctions" or "titres de séjour ID card" as soon as they are employed by CPVO. They are also requested to supplement information in the "Fiche Individuelle" and "Notification de Nomination et de Prise de Fonctions". Simultaneously, they are informed that the "Protocole sur les privilèges et immunités des Communautés Européennes", which is made available in the Intranet of the Office, Sharepoint.

The Privacy Statement is also made available to the data subjects in the intranet of the Office, Sharepoint.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

For the processing operation, the subsequent data is collected:

- Identification data: title (M., Mme or Mlle), name (and maiden name for married women), place of residence in France, former place of residence, number of the actual titre de séjour special (in case of a replacement), date, place and country of birth, nationality (specifying if acquired by birth, marriage or naturalisation); Signatures and photos are also collected;
- Passport information: type, number, place of validation and expire date;
- Visa information (if applicable);
- Date of arrival in France and date when post was taken up in France;
- Contact information: personal address in France and last personal address;
- Whether the applicant has or not double French nationality;
- Relatives' personal information: spouse (including: name, gender, date and place of birth, nationality, date of marriage, and country of residence), parents (name, surname and date of birth) and children (name, surname and date of birth);
- Administrative status: place of work, staff category and professional position; last place of work (city, country, last designation);
- Marital status: marital status, identity of spouse or ex-spouse, date and place of wedding, data related to the change of marital status.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The data is available in electronic copies and stored in the personal files of each staff member concerned, in Docman (electronic storage of documents), in the staff member's personal file. Physical copies of the files may also be stored in paper in cupboards at the premises of the Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Only the HR sector has access to all the personal data processed. In addition, also the IT Administrators and the President, who is the responsible for signing the form "notification de nomination et de prise de fonctions" and the French Ministry of Foreign Affairs may have access to the data processed on a *need-to-know-basis.*

15. * Period of retention for the data:

In accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member. The end of contract can be due to a contract with a limited duration, dismissal, resignation, retirement or death of the staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organization.

17. * Measures to ensure security of processing:

Appropriate technical and organisational measures are implemented in order to safeguard and protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to it. All documents provided are kept in the CPVO premises which are safeguarded by the security team of the Office. The servers are also kept in house, in locked rooms, and are password protected and accessible only by authorized staff members. Other security members include IT layered security, including firewalls.

Regarding physical copies of personal files, these are locked in a filing cabinet and only the HR sector (and its' replacement) has the key. Access to Docman is secured by a username and password and only staff members of the Human Resources sector and the IT Unit members have access to these documents on a *need-to-know* basis.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Appointment of Middle Management staff

2. * Last update of this record:

19/03/2021

3. Reference Number:

No 3

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit

External processors:

Kioskemploi (and its sub-processors)

7. Description of the processing operation:

The processing operation concerns the appointment of middle management staff members.

For officials, the President may decide to fill the post by publication pursuant to Article 29 of Staff Regulations:
- If the post is advertised internally or inter-institutionally, the President publishes the post at a range of grades corresponding to the functions;
- If the post is advertised externally, the President publishes at one grade out of the grades AD9 to AD10.

For temporary agents, the President may decide:
- To advertise the post simultaneously in the Agency and in the Interagency Job Market, before making an external publication of the vacant post. Applications of the internal candidates are considered first, before the applications of the candidates of the Interagency Job Market.
- To publish externally and to launch a selection procedure in accordance with the decision on the engagement and the use of temporary agent for temporary agents who are recruited through an external selection procedure.

After the Training, a trial period of 9 months follows, after which a final assessment is drawn up.

When the post is advertised internally (and inter-institutionally), applications can be made through e-recruitment platform GestMax, an online application software system provided by "Kioskemploi", and some information may also be sent by email. When the post is advertised externally, then applications are made through the Contractor's platform (Gestmax).

8. * Purpose(s) of the processing and legal basis:

The processing activity is necessary to manage the selection of middle management staff for positions ranging from grade AD9 to AD12.

Legal Instruments:

- Articles 2, 4, 5, 7, 29, 34, 43 and 44 of Staff Regulations;
- CPVO Administrative Council Decision on Middle Management based on Commission Decision C(2018) 2542 of 24 April 2018 on giving the Commission's ex ante agreement to the adoption by decentralized agencies and joint undertakings on implementing rules on middle management staff on 19 September 2019;
- CPVO Internal Procedure of 15 January 2013 to be followed in CPVO recruitments.

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Officials and Temporary Agents of EU institutions (internal candidates) and, in some cases, external applicants.

10. When and how were data subjects informed:

A Privacy Statement is made available in the CPVO's website along with the call for applications.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data processed are:

- Identification data, including name, surname, date and place of birth, nationality, telephone number, email address, correspondence address; military status (and grade);
- Education and professional experience, including the degree/diploma, date of award of degree, length of professional experience, length of management experience, languages spoken and level, previous working experience and personal reference number (if applicable);
- Data related to the suitability of a candidate for a vacancy, including the assessment/grids by the pre-selection panel as regards the eligibility of the candidate, the matching of the application with the selection criteria and the performance during the interview(s) and previous assessment reports;
- Photos can be collected, on a voluntary basis.

From the Management Probationary Period Report the following data is collected:
- Identification data from reporting officers, including name and surname, institution, staff number, function.
- Personal data of the appraisee, including name and surname, category, grade and function.

12. Procedures to grant data subjects' rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu by *explicitly* specifying *the request*.

13. Storage media of data:

At the CPVO, information is stored in electronic form internally and it is password-protected. Documents with relevant data may also be kept in hard copies in locked cupboards.

As regards the service provider Kioskemploi, data are stored in the online platform GestMax. Data is stored within the European Union.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal Recipients:

- Human Resources sector;
- Selection Committee;
- Reporting Officers;
- Accounting sector for the purpose of payments of individual entitlements (only for successful candidate).

External Recipients:

- Kioskemploi (and its sub-processors).

15. * Period of retention for the data:

As regards unsuccessful candidates and in accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, data from unsuccessful candidates kept on paper or in electronic format by the Human Resources sector will be destroyed after a period of 2 years from the date of decision of the Office appointing the successful candidate.

Regarding working documents, in paper or electronic format, which are used by members of the Selection Committee appointed for recruitment procedures in the CPVO, these shall be destroyed once the selection procedure is closed, that is, on the date of the decision of the CPVO appointing the successful candidate.

As regards successful candidates, in accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, the data collected during the middle management procedure are kept in the personal files and will be destroyed after a period of 10 years from the date of the end of the contract of the staff member.

As regards data processed by the external service provider Kioskemploi, data will be retained for no more than two years from the end of the selection procedure.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organisation.

17. * Measures to ensure security of processing:

Files containing applications and evaluation reports are locked in cupboards at the premises of the Human Resources sector. Access to internal storage is password-protected. The controller ensures that the data collected are processed only by authorised staff members based on the *need-to-know* principle.

Regarding the external service provider Kioskemploi and its sub-processors, these implement appropriate technical and organisational measures, to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Measures are in place to protect the confidentiality of the data stored on the service provider's platform GestMax.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Engagement of Temporary Agents

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 4

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources Sector)

External processor:

Kioskemploi
Kioskemploi sub-processors

7. Description of the processing operation:

The selection procedure for recruiting Temporary Agents for CPVO vacancies can be carried out in two ways:

- Either the European Communities Personnel Selection Office (EPSO) organises, on request of the CPVO and in accordance with Article 3.1 of Decision on Temporary Agents in the CPVO of 8 December 2008, a selection procedure, where EPSO provides the CPVO with a short list of successfully tested candidates, which the CPVO then invites for interviews.
- Either the CPVO organises by itself the selection procedure in accordance with Articles 3.2, 3.3 and 4 of Decision on Temporary Agents in the CPVO of 8 December 2008.

The selection procedure for Temporary Agents in the CPVO consists of the following steps:

- The Selection Committee, composed of 3 to 5 members (including a reporesentative of the Staff Committee nominated by the President), shall first meet to determine the details of the vacancy notice, the eligibility criteria and the selection criteria. They shall also specify the thresholds, the content and the organisation of interviews and tests.
- The vacancy notice is published via official means (e.g.: CPVO web site, EPSO, Interagency job market);
- Candidates submit their applications with a detailed CV, the application form filled in, and a motivation letter to the Human Resources sector via Gestmax recruitment portal;
- The Human Resources officer/assistant acknowledges receipt of the application using a standard e-mail via GESTMAX indicating the selection candidate number;

- Once the deadline for applications has elapsed, all the applications are shared with each member of the Selection Committee, through e-mails and GestMax or in SharePoint, in a folder with restricted access;
- The Selection Committee members evaluate the applications received and select those meeting the eligibility and the selection criteria required as per vacancy notice;
- The Selection Committee invites the selected candidates to written tests and interviews. Minutes of the Committee meetings shall be drawn up setting out the reasons for any decisions taken;
- Candidates bring original documents and paper copies when invited for the interviews and the tests. The original documents are given back to the candidates and the copies are certified conform to the originals by Human Resources sector;
- After the completion of the tests and interviews, the Selection Committee shall propose a list of successful candidates to the Authority empowered to conclude contracts of employment, who may establish a reserve list of successful candidates. Candidates shall be informed of the outcome of the written tests and interviews, as well as the enrolment to the reserve list.
- The Authority empowered to conclude contracts of employment will choose the final successful candidate on the reserve list.

8. * Purpose(s) of the processing and legal basis:

The processing of personal data is necessary in order to evaluate and select candidates for vacant Temporary Agents posts within the CPVO.

Legal Instruments:

- Articles 2 and 15 of the Conditions of Employment of Other Servants;
- CPVO Decision of 8 December 2008 on Temporary Agents in the CPVO;
- Internal Procedure to be followed in CPVO recruitments of 15 January 2013;
- SLA Agreement of 7 April 2017 between the CPVO and Kioskemploi.

Legal Basis:

Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Candidates for Temporary Agent vacancies in the CPVO.

10. When and how were data subjects informed:

The Privacy Statement is published along with the vacancy notice on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following personal data are processed for each candidate:
- Candidate reference number;
- Name and Surname;
- Title;
- Date and Place of birth;
- Nationality;
- ID card or passport;
- E-mail address;
- Phone number;
- Postal address;
- CV, including knowledge in languages, educational background, and professional experience.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit dpc@cpvo.europa.eu by *explicitly specifying* the request.

13. Storage media of data:

Documents sent by the candidates when applying are stored in the GestMax database of the sub-processor Kioskemploi.

In the Intranet of the Office, SharePoint, for each published post a specific folder is created with an access restricted to the members of the Selection Committee as well as to selected Human Resources representatives. Paper documents received from the candidates coming to the interviews are stored in sealed envelopes and locked in a cupboard at the premises of the Human Resources.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data are disclosed to the following recipients on a *need-to-know* basis:

Internal recipients:

- The Human resources sector;
- Selected members of the Staff Committee;
- the Authority empowered to conclude contracts;

External recipients:

- Kioskemploi and its sub-processors.

15. * Period of retention for the data:

In accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, Data from unsuccessful candidates kept on paper or in electronic format will be destroyed after a period of 2 years from the date of decision of the Office appointing the successful candidate. As regards sucessful candidates, the data collected during the selection procedure are kept in the personal files and will be destroyed after a period of 10 years from the date of the end of contract of the Temporary Agent staff member.

Regarding working documents, in paper or electronic format, that are used by the members of the Selection Committee appointed for recruitment procedures in the CPVO, these shall be destroyed once the selection procedure is closed, that is, on the date of the decision of the CPVO appointing the successful candidate.

As regards the external processors Kioskemploi, data are retained for two years after the end of the selection procedure.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Access to the platform GestMax by CPVO staff members and access is usename and password protected. Access through login is restricted to the Human Resources sector. The files containing the applications are locked in cupboards in the Human Resources member's. The specific folders in the CPVO Intranet, SharePoint, have a strict access policy limited to the nominated Selection Committee members and selected members of the Human Resources sector

As regards the external service provider, Kioskemploi and its sub-processors implement appropriate technical and organisational measures, in order to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Measures are in place to protect the confidentiality of the data stored on the service provider's platform GestMax.

Only authorised staff members of Kioskemploi and Kioskempoli sub-processors may access remotely the servers and the data. Access to servers of Kioskemploi are secured and protected by a firewall.

Kioskemploi monitors on a daily basis any flaws identified in the tools in place and conducts as well a more comprehensive review a few times per year.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Reimbursement of Travel and Subsistence Expenses of Candidates to a CPVO vacancy

2. * Last update of this record:

20/03/2021

3. Reference Number:

No 5

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of processor:

Administration Unit (Human Resources Sector)

7. Description of the processing operation:

In accordance with the "Provisions on a Financial Contribution towards travel and subsistence expenses", a financial contribution towards travel and subsistence expenses shall be granted to any candidate invited to written and/or oral tests of a selection procedure of the Office, to a subsequent interview, or to a pre-recruitment medical examination.

When inviting the candidates to take part in tests, interviews and/or a medical examination, the form to be filled in for the reimbursement request and the financial identification form are sent to the candidates. Once the tests, interview and/or medical examination have taken place, the candidates return the forms duly completed and signed with the original travel documents. The reimbursement is then carried out.

8. * Purpose(s) of the processing and legal basis:

Personal data are processed in order to reimburse all the expenses incurred in by the candidates invited for written and/or oral tests of a selection procedure, to an interview or to a medical examination.

Legal Instruments:

- Provisions on a Financial Contribution towards travel and subsistence expenses for persons invite to the written and/or oral tests of a selection procedure, to an interview or to a medical examination of 3 November 2009;
- Internal Commission Directive N° 06-2018 of 27 February 2018 (Conclusion No 277/17 – Rules on financial contributions towards travel and subsistence expenses for persons invited to tests organised as part of a competition or selection procedure, or to an interview or medical examination);
- Article 42(5) of the Financial Regulation of the CPVO and Article 21(d) of its Implementing Rules.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Candidates who are invited to written and/or oral tests of a selection procedure, to an interview or to a medical examination.

10. When and how were data subjects informed:

When invited to the written and/or oral tests of a selection procedure, to an interview or to a medical examination, the forms to be filled in as well as a copy of the "Provisions on a Financial Contribution towards travel and subsistence expenses" are sent to the candidates.

The Privacy Statement is sent to data subjects and published as well internally on the Internal SharePoint of the Office.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected refers to the vacancy, the travel arrangements and the bank account information, including:
- Reason for the reimbursement (competition, interview, or medical visit);
- Selection reference and interview date;
- Candidate's personal details: name, surname, e-mail address, postal address, city, town, postcode;
- Bank account information: name and address of the bank, IBAN number, account number, swift code;
- Signatures from the candidate and from the bank representative (with the bank stamp) (this is not necessary if a recent bank statement is enclosed with the financial identification form);
- Travel arrangements: travel itinerary and means of transport.

Data is also collected from the original travel documents, which must be sent to the Administration Unit.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The Data Subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The digital copies of the data are stored in the Internal database of the Office "Docman", and hard copies are also locked in cabinets of the Office and only authorised staff members of the Administration Unit have access to it.

14. The recipients or categories of recipients to whom the data might be disclosed:

The Human Resources service has access to the personal data processed under the present processing activity. Financial assistants in the Accounting and Financial Service have also access to personal data necessary for the payments required. The IT Unit may have access as well to the data on a *need-to-know basis*.

15. * Period of retention for the data:

In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not transferred to any third country or international organisation.

17. * Measures to ensure security of processing: Access to Docman is secured by a username and password for access by the concerned recipients. The servers are password-protected and kept at the premises of the Office locked in rooms. An inbound firewall protects the system against incoming traffic and an outbound firewall protects against outgoing traffic. The premises are safeguarded by the Security team of the Office.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the Privacy Statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Payment of Monthly Remuneration to staff

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 6

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector; Accounting and Finance sector) and Autorising officers.

External processor:

SYSPER 2 (European Commission);
PayMaster Office (PMO) (European Commission).

7. Description of the processing operation:

Throughout the career of a CPVO staff member, data related to remuneration and allowances are collected. In accordance to Article 62 of the Staff Regulations of Officials, remuneration shall comprise basic salary, family allowances and other allowances.

In order to receive the remuneration, newly recruited staff members must fill in at the latest at their entry into service two PayMaster Office (PMO) forms. These data are also registered in SYSPER in modules PER (personal data) and FAM (data related to their family).

The Human Resources sector sends the two forms by e-mail to the PMO. The PMO, being delegated AIPN for individual entitlements, validates the individual elements which are then presented to the staff member concerned so that he/she can confirm the information and sign the forms. After this validation, each staff member is responsible for the update of his/her own data according to the changes occurring in his/her family or personal situation. Declaration forms for these changes are available in SYSPER. The PMO will use these data for the calculation of the remunerations of all staff members.

Every month, the Human Resources sector downloads the documents in relation to the salaries from a dedicated and securised platform of the Commission (BI4). HR checks the information and then stores it on its computer and in the internal database Docman. The documents can only be accessed by the Human Resources sector, the accounting officer and the subordinate accountant, by the authorising officer, which usually is the Head of the Administrative Unit and in his absence, by the President or the Vice-President.

Once all the above information is checked by the Human Resources sector, a payment order is created for each staff member (including the bank account information and the amount to be paid).

Every month, the data subject can download his/her detailed salary statement from SYSPER with the corresponding amount of remuneration, allowances and the amount of taxes deducted.

8. * Purpose(s) of the processing and legal basis:

The processing of the data is necessary for the purposes of handling the procedure for the remuneration to which data subjects are entitled.

Legal Instruments:

Article 62-71 and Annex VII of Staff Regulations of Officials;
Articles 19-27 and 92-94 of Conditions of Employment of Other Servants (CEOS).

Legal Bases:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);
- Article 5.1 (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

All staff having a statutory contract with the CPVO.

10. When and how were data subjects informed:

All along with the information provided as to the remuneration to which the data subjects are entitled, the data subjects are informed about the privacy statement concerning this particular processing, which is available in the Intranet of the Office, Sharepoint, Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The processed data are the following:

- Personal Reference Staff number;
- Name and Surname;
- Date and place of birth;
- Nationality;
- Gender;
- Category, grade and step of the post;
- Number of children, their age and education status;
- Marital status;
- Identity and employment of the official partner;
- Places of residence for the last 10 years;
- Previous employments for the last 10 years;
- Place of origin;
- Bank details, including name and address of bank, account number, IBAN, swift;
- Postal address;
- Amount to be paid (basic salary, all kind of statutory allowances, retentions for any reasons, illness, accident, insurance, transfers of part of salary, etc.).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The Data Subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The personal data (including grade and step, administrative status, civil status, place of origin and nationality, etc) is filed in the internal database Docman, in the individual staff folders. The data are also stored on paper in the personal files dedicated to each staff member under locked cupboards at the premises of the Human Resources sector. The payslip is available for each staff member in SYSPER. A copy of this PDF document is stored on the Human Resources server and in Docman.

The financial data are stored in the accounting database EPM/PIA with a restricted access for staff of the Accounting and Finance sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Access to the personal data is provided to the CPVO and Commission Staff responsible for carrying out this processing operation and authorised persons according to the *need-to-know* principle.

Internal recipients:

Staff of the Human Resources sector, the Accounting officer and the subordinate accountant, the Authorising officer, which usually is the Head of the Administrative Unit and, in his absence, the President or the Vice-President.

External recipients:

The data is accessed by the relevant staff in the Paymaster Office (PMO) (European Commission).
For more information, please refer to Record No 68 SYSPER.

15. * Period of retention for the data:

In accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data on paper will be destroyed after a period of 10 years from the date of the end of contract of the staff member, apart from the administrative data which are stored in the pension part of the personal file.

The data stored in SYSPER is kept and used by the PMO as long as the staff member will receive a pension amount and according to the rules on retention applied by the Commission. For more information, please refer to Record No 68 SYSPER.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not transferred to a third country or international organizations.

17. * Measures to ensure security of processing:

The physical personal files are locked in a cupboard and only the relevant staff of the Human Resources sector has access. Access to Docman is username and password-secured and only authorised staff members have access to these documents. Such persons are bound by their statutory obligations under the Staff Regulations.

The security measures linked to SYSPER are described in Record No 68 SYSPER.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with an asterisk* are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Promotion and Reclassification of Officials, Temporary Agents and Contract Agents

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 7

4. * Name and contact details of the Controller:

Head of Administration
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources Sector)

External processor:

SYSPER 2 (European Commission)

7. Description of the processing operation:

The processing relates to the promotion/classification system applicable at the CPVO, more precisely, to the promotion of officials (with the exception of those in a grade higher than AD13), to members of the contract staff employed under Article 3a of the CEOS, and to the classification in the next higher grade (reclassification) of temporary staff referred to in Article 2(f) of the CEOS (with the exception of those in a grade higher than AD13).

The promotion/reclassification system is based on consideration of the comparative merits of the officials eligible for promotion, taking account of the reports on the officials, the use of languages in the execution of their duties other than the language for which they have produced evidence of thorough knowledge and the level of responsibilities exercised by them. Promotion entails the appointment of the official concerned to the first step of the next higher grade in the function group to which he or she belongs.

The promotion/reclassification exercise is launched, once the appraisal exercise organised in the same year has been finalised, based on the Annual Career Development Report (CDR) that is managed in the IT tool "Centurio". At the start of the promotion/reclassification exercise, the Human Resources sector informs the President. The President, Vice President, and Heads of Unit, proceed with the examination of the comparative merits of the officials/agents eligible for promotion/reclassification. Following this examination, the President holds a discussion with the Staff Committee. He subsequently draws up a list of officials/agents proposed for promotion/reclassification.

The President then communicates to all CPVO staff members the list of the officials/agents he wishes to propose for promotion/reclassification and shall forward this list to the Joint Promotion and Reclassification Committee (Joint Committee).

Officials/agents have ten working days from the date of publication of this list in which to lodge a complaint with the Joint Committee against the fact that he or she is not on the list, with supporting arguments. On receipt of the list, the Joint Committee, taking into account any complaints it has received, shall compare the merits of the officials/agents eligible for promotion/reclassification and present for the attention of the President the list of officials/agents it recommends for promotion/reclassification.

Once the President has received the information from the Joint Committee, and has at his disposal the files of all the officials eligible for promotion/reclassification, he carries out a final comparison of the merits of the eligible officials/agents. Taking into account the budgetary resources available, the President adopts the list of officials/agents promoted.

The list of officials/agents promoted/reclassified is finally made available to all CPVO's staff by means of a notice. Promotions then take effect on 1 January of the year of the promotion.

Part of the processing operation is carried out in SYSPER, more precisely, under module CAR. For more information, please refer to Record No 68 SYSPER.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is to enable the taking of decisions about the promotion/reclassification of CPVO staff members (Officials, Temporary Agents and Contract Agents), based on the average career plan and on the general assessment of staff as reflected in the Annual Career Development Report (CDR).

Legal Instruments:

- Articles 45 and 46 of Staff Regulations;
- Articles 45, 54, and 87(3) of the Conditions of Employment of Other Servants of the European Union (CEOS);
- CPVO Decision of 17 June 2016 on reclassification for temporary staff;
- CPVO Decision of 17 June 2016 laying down general implementing provisions regarding Article 45 of the Staff Regulations on promotion rules for officials;
- CPVO Decision of 17 June 2016 laying down general implementing provisions regarding Article 54 of the Conditions of Employment of Other Servants of the European Union;
- CPVO Decision of 17 June 2016 on general implementing provisions regarding Article 87(3) of the Conditions of Employment of Other Servants of the European Union.

Legal Basis:

- Article 5(1)(a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).
- Article 5(1)(c) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Officials, Temporary Agents, Contract Agents).

10. When and how were data subjects informed:

The Privacy Statement is available on the Intranet of the CPVO, Sharepoint, under the Data Protection Officer section. CPVO internal decisions on promotion and reclassification rules for Officials, Temporary Agents, and Contract Agents, respectively, are also made available in Sharepoint.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Through the Annual Career Development Report (CDR), the following data are collected:
- Name and Surname;
- Personal Number;
- Current Grade;
- Period covered by the CDR;

- Job Description (including job title, purpose of the job, main work areas/responsibilities in order of importance, plus % time allocated to each area and resources managed);
- Reporting Officer's Assessment (including achievement of work objectives for the period, achievement of personal development objectives for the period, assessment of performance against criteria);
- Information concerning the ability to work in a third language (in accordance with the general rules);
- Overall assessment of the jobholder's performance;
- Other report(s).

Through the eligibility for promotion/reclassification table, the following data are collected:
- Name and Surname;
- Current Grade;
- Date of entry to current grade;
- Starting date/last promotion/reclassification date;
- Promotable year (according to the Staff Regulations);
- Average Career Plan (in years).

Through the CPVO Decision on promotions/reclassifications, the following data are collected:
- Name and Surname.

Through the Reporting Officer's Assessment, the following data are collected:
- Name and Surname.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The paper copies of the final CDR and the promotion/reclassification decision are kept in the personal file of the Official, Temporary Agent, or Contract Agent inside locked cupboards of the Human Resources sector.

The electronic files are stored in the internal database Docman and the CDR reports in the virtual servers of IT tool Centurio.

The promotion/reclassification eligibility tables are also stored in the professional device of the Human Resources staff member.

14. The recipients or categories of recipients to whom the data might be disclosed:

The data may be disclosed to the following recipients on a *need-to-know* basis:

Internal recipients:

- President, Vice-president, Head of Unit for staff for whom they serve as supervisors, appeal assessor and countersigning officer (if it is the case);
- Joint Committee, Staff Committee;
- All CPVO staff members, prior to launching a promotion or reclassification exercise, can have access to Names and Surnames of eligible staff members and date of entry into current grade, as published internally.

External recipients:

- SYSPER 2 (European Commission)
- DG DIGIT (European Commission)

15. * Period of retention for the data:

In accordance with the CPVO Decision on Retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data, including evaluation reports, decisions on promotion and reclassification, will be destroyed after a period of 10 years from the date of the end of contract of the staff member. As for Carrier Development Reports (CDRs), these will be destroyed after a period of 10 calendar years (for example, CDRs of 2021 will be destroyed on 1/1/2032). Concerning documents stored in SYSPER, please refer to Record No 68 SYSPER.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not transferred to any third country or international organization.

17. * Measures to ensure security of processing:

Access to Docman is password-secured and only the concerned recipients on a *need-to-know* basis have access to documents relevant to the procedure. The same applies to files stored in the virtual servers of IT tool Centurio.

The paper copies of the final CDR and the promotion/reclassification decision are kept in the personal file of the Official, Temporary Agent, or Contract Agent, inside locked secured cupboards at the premises of the Human Resources sector. Only the concerned staff member and the Human Resources staff members can access the data.

The data recipients involved in the promotion/reclassification procedure, are also bound by a confidentiality agreement. For instance, members of the Joint Promotion and Reclassification Committee are under the duty to keep confidential the deliberations and documents used for the purposes of the procedure.

Regarding documents containing personal data processed in SYSPER, please refer to Record No 68 SYSPER.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Management of Training Courses for staff

2. * Last update of this record:

05/04/2021

3. Reference Number:

No 8

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Human Resources sector (training manager)

External processors:

Training companies

7. Description of the processing operation:

The processing operation consists in the offering to CPVO staff members of trainings that help them in acquiring or developing new knowledge or skills in key areas for their performance of their tasks. A staff member wishing to follow a training course agreed with his/her reporting officer either within his/her CDR (Development Plan for the year) or on an *ad-hoc* basis has to apply for a course using the CPVO tool to request training (Centurio). Applications shall be approved by the relevant Head of Unit.

If the staff member undertakes to follow training activities on his/her own initiative, the Head of Unit shall give his/her opinion on the value of the training in respect of the CPVO interests, subject to the final approval by the CPVO President. The President shall approve it. It that case the training is organised by the staff member. Applications should be filled in at least 1 month before the period foreseen for the training or before the final enrolment date.

Once the application is approved by the relevant Head of the Unit, the personal data, such as name, surname, email, could be disclosed to the training company, responsible for providing the certain training, in order to contact the staff member concerning the training and issue a certificate of the attendance in the end of course. Training courses could be intra or inter.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is to manage the requests from CPVO staff members to attend training courses, with a view to enhance the knowledge or skills of staff members in key areas for the performance of their tasks.

Legal Instruments:

- Articles 24(a) and 45(2) of the Staff Regulations;
- Articles 11 and 85(3) of CEOS;
- CPVO training policy of 26 June 2014.

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

All CPVO staff falling under the Staff Regulation and the CEOS, including Seconded National Experts.

10. When and how were data subjects informed:

The Privacy Statement is available in the register of data processing activities under the Data Protection Officer section in the Intranet of the Office, Sharepoint.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Data subjects are requested to provide the following data, when applying for the training course via "Centurio":
- Nature of the training: language, duration of training, type of request;
- Reasons for attending the training;
- username and password;

The following data could be provided to the external processors (training companies):
- Name, surname;
- Email;
- In case a certificate is to be issued, also ID number, birthdate and place of birth.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, dpc@cpvo.europa.eu by *explicitly* specifying *the request*.

13. Storage media of data:

Electronic copies of documents containing personal data are stored in Docman and Centurio. The certificate of attendance is stored in the personal file of the staff member.

As regards training companies, most customer data is kept in Europe, but additional data may be made available to subcontractors in other countries (see point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Access is granted to internal and external recipients on a *need-to-know* basis.

Internal recipients:

- Head of Administration Unit, the Head of Unit of the staff member concerned, the training manager, the HR sector;
- Accountancy sector for the purpose of managing invoices;
- IT System Administrator for the purpose of maintenance of Docman database.

External recipients:

- Training companies and their sub-processors.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

As regards service providers, the retention period varies in relation to the training company processing the data on behalf of the Office.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations outside the recipients and the legal framework. However, the service provider EFE Formation may make available personal data to a sub-processor established in Mauritius. The transfer is governed by Standard Contractual Clauses approved by the European Commission.

17. * Measures to ensure security of processing:

Personal data is stored in secure IT system according to the security standards of the CPVO. Access to Docman is username and password protected. Access is restricted to the training manager, the Human Resources sector, the Accounting sector and the IT administrators. Access to staff members' applications for training courses in Centurio is given only to the Head of Unit of the staff member concerned, the training manager and the Human Resources sector. All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

The training companies have put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Mail Services Management

2. * Last update of this record:

26/03/2021

3. Reference Number:

No 9

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Legal, Procurement and Logistics (P&L)

External processors:

La Poste
DHL International Express France

7. Description of the processing operation:

The Mail Management (MM) services of the Office, concern the management of mail courierrs or parcels delivered in by the services of La Poste or by DHL, transporters, and of e-mails from the e-mail central mailbox cpvo@cpvo.europa.eu. The CPVO has signed mail and parcel delivery contracts with La Poste France (Affranchigo Forfait) and a with DHL International Express France. Within the framework of these contracts, La Poste and DHL may collect personal data from the CPVO in order to carry out transport/logistic services.

The management of the mail is carried out by Procurement and Logistics (P&L) with input from the CPVO Security Guards.

The CPVO Security Guards carry out the following tasks:
- They are in charge of reception of mail deposited by the post service early in the morning and by the express service providers received all day long and hand delivered couriers at the reception, and have to inform P&L upon receipt of express mails;
- Collection of potential mail in the external mailbox;
- Counting and filling in the mail summary table (available at the CPVO reception);
- Separation of newspapers, magazine, and advertisements from envelopes (without opening them);
- Affixing the "stamp date" on each envelope;
- Provision of paper mail in the "IN bin" in the reception cupboard.

Procurement and Logistics is responsible for the handling, digitalising and sorting of all incoming

correspondence (i.e., mails/parcels that are delivered directly or sent by fax or post to the Office). In particular, P&L is responsible for the following tasks:
- Opening incoming paper mail placed by the Security Guard in the "IN bin" in the closet located in the main entrance of the CPVO "HBM" building;
- Separation of official, confidential and personal envelopes and allocation to each units and/or services in the "sorter" (if the words "Personal" or "Confidential" are entered, the envelope will not be opened);
- Provision to the CPVO Security Guards of the "sorter" for the distribution of correspondence in the thre buildings of the Office.

P&L is also in charge of handling all outgoing Office correspondence by post or courier service provider (La Poste/DHL), as well as of digitalizing incoming emails from the CPVO mailbox.

8. * Purpose(s) of the processing and legal basis:

The purposes of the processing operation are the ensurance of sustainable, timely and quality management of CPVO correspondence.

Legal Instruments:

- Article 30 of Council Regulation (EC) No 2100/94 on Community plant variety rights;
- Article 64 of Commission Regulation (EC) No 874/2009 on proceedings before the CPVO;
- CPVO Internal Procedure: Gestion du Courrier et des emails de la boite de reception of 31 March 2021.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Data subjects are both internal staff (such as Permanent Officials, Temporary Agents, Contract staff, Seconded National Experts, Interim Agents and trainees) and external users.

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects in the intranet of the Office, "Sharepoint", under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data processed are the following:

- Identification data such as name, internal Office ID number and contact details (email, address, telephone number);
- Regarding the post and courrier service provider La Poste and DHL, these process only name, address and telephone number;
- Financial data such as bank accounts to debit/link payments;
- Data contained in applications for Community Plant Variety Rights (CPVRs) and CPVR granted titles.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Legal Service, to the e-mail address dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Digital data is stored in the CPVO Internal Database "Docman", and data in paper is stored in archives (depending on the concerned Unit/Sector with which correspondence is exchanged, they will be stored in the corresponding archives for which the concerned Unit/Sector is responsible).

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- CPVO Staff members.

External recipients:

- Senders of correspondence;
- La Poste/DHL in the framework of the management of outgoing correspondence by post or courier.

15. * Period of retention for the data:

In accordance with the CPVO Internal Procedure "Destruction of Paper Documents stored in five specific profiles" of 26 November 2018, where electronic files have been generated on the basis of paper documents, the original paper copies are destroyed by P&L after a period of three years. This procedure is carried out annually (in March).

Regarding digital copies of data stored in Docman, the duration of the retention period for the data will depend on the subject matter covered and the Unit/Service concerned, to which a specific retention period applies in accordance with the concerned CPVO internal decision and/or procedure.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

For the provision of certain services, La Poste may resort, to sub-processors outside the European Economic Area (Morocco, India, Sénégal, Tunisia, Mauritius Island and United States). La Poste ensures that the sub-processors provide sufficient data safety guarantees by signature of the Standard Clauses set by the European Commission or by the adoption of Binding Corporate Rules. For more information, please refer to the Data Protection Policy of la Poste, available here.

As regards DHL (France), data may also be transferred to third countries. Safeguards are put in place by DHL by means of Binding Corporate Rules to guarantee an adequate level of protection in those countries. For more information, please refer to the Data Protection Policy of DHL (France), available here.

17. * Measures to ensure security of processing:

The CPVO has in place a number of technical and organisational security measures. These include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. CPVO staff members are also required to sign a confidentiality declaration at the time of signature of their employment contract with the CPVO.

Personal data in digital documents is stored in secure IT Systems at the CPVO. For instance, access to the internal database Docman is username and password-protected. As for paper files containing personal data, these are kept in locked cupboards at the premises of the concerned CPVO Unit/Service.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Pre-employment and Annual Medical Visits

2. * Last update of this record:

29/03/2021

3. Reference Number:

No 10

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processors:

- Dr Stievenard at the "Cabinet médical d'Avrillé" to outsource the pre-employment medical visit and the annual check-up of the CPVO staff members;

- Dr Buisson and Jobard from the "Cabinet d'Ophtalmologie d'Avrillé" for the eyes' tests required in the pre-employment medical visit and the annual check-up of the CPVO staff members;

- "Laboratoire d'Avrillé" for urine and blood tests required in the pre-employment medical visit and the annual check-up of the CPVO staff members.

7. Description of the processing operation:

Pursuant to Article 28(e) of Staff Regulations of Officials (ensuring that the staff member appointment is physically fit to perform his/her duties), the CPVO organises a pre-employment visit with its contracting doctors. Employment contracts with the CPVO state that "the contract is concluded under the suspensive condition of a positive result of the pre-employment medical visit". In case of negative medical report, Article 33 of Staff Regulations of Officials applies.

For candidates who successfully pass a competition for a position at CPVO, the pre-employment checks are, as a general rule, organized by the CPVO with the three contracting parties. However, on request, a successful candidate can be authorized to make the pre-employment check with another medical examiner of one of the Institutions/bodies.

Within the pre-employment medical visit procedure, the candidate takes a physical examination and the physician completes a medical "overview form" with medical information given by the candidate. Regarding the physical examination, this consists in a chest X-ray and an electrocardiogram test, as well as in a series of laboratory examinations on the candidate's blood, urine and stool samples. Regarding the medical "overview form" requests certain additional information about medical problems, such as

menstruation, "family situation" and eventual problems of psychological or psychiatric nature, "lifestyle" questions. Under "conclusions" the physician may give his views for a possible treatment or follow-up.
In addition to the standard medical check-up, if necessary, the physician may require that the candidate takes complementary exams. Furthermore, within the remit of the Office, CPVO staff members also undergo an eye examination performed by the ophthalmologist.

All data are collected and kept by the contracted physicians, that is, no details on the medical status of the concerned staff member are transferred to the CPVO. In the pre-employment check procedure, the Human Resources sector only receives and stores the certificate of fitness (and has no access to the medical details) in the personal file of the staff member. The certificate of fitness is a form attesting the physical suitability/partial suitability or non-suitability of a candidate to fill the vacant post.

The annual check-up follows the same procedure and the data collected is the same as for the pre-employment visit. The Human Resources sector keeps a form attesting that the CPVO Staff Member undertook the annual check-up.

Data subjects may choose to have their annual medical check-ups done with another medical centre or doctor, other than the one with which the Office has a contract and which the Office recommends. Also, personal medical data may be transferred by another EUI to the CPVO (that is, where a Staff Member changes employment from one EUI to another EUI).

The contract between the CPVO and the Doctor provides for the possibility for the CPVO to request additional medical visits as provided for in Article 59(1) 3rd paragraph of the Staff Regulations of Officials.

The CPVO statutory staff members (Officials, Temporary and Contract agents) then make requests to the Human Resource Sector to get reimbursement for the expenses they may have incurred in relation to the obligatory pre-employment medical visit or annual medical visit. This request is made by writing a simple memo stating what exams he/she had undertaken and its costs. All the original supporting documents shall be attached to the memo. In order to create a document for reimbursing expenses SIFI system is used. The employees of the Human Resources sector may maintain requests for reimbursements resulting from pre-employment medical check-ups and annual medical check-ups.

8. * Purpose(s) of the processing and legal basis:

The personal data collected in the framework of the pre-employment visit and annual check-up procedures are necessary to ensure the efficient management and functioning of the CPVO. The purpose of the pre-employment and annual visit are carried out to determine whether a candidate is fit for the work.

More specifically, the medical examination before appointment is intended to determine physical fitness for employment in any of the European Union Institutions and Bodies and determine the entitlement to guarantee benefits in respect of invalidity or death.

The medical results are not used to assess health insurance risks. In particular, they are not used to determine whether the candidates will be entitled to health insurance benefits or what will be the amount of health insurance payable. This is with two exceptions:

- the CPVO may apply to candidates the Article 1 of Annex VIII of the Staff Regulations (and Article 32 and 100 of the Conditions of Employment of Other Servant (CEOS)) which allows the appointing authority to limit, for a maximum of 5 years, the benefits in case of death or invalidity due to a pre-existing condition.

- the CPVO may invoke the second paragraph of Article 28 of the CEOS which is applicable only to Temporary and Contractual Agents and allows the appointing authority to deny any medical coverage to a Temporary or Contractual Agent for pre-existing illnesses.

A further purpose of the present processing is to manage and ensure that the reimbursement of the medical expenses resulting from pre-employment medical check-ups and annual medical check-ups.

<u>Legal Instruments:</u>

For Pre-employment visits:

- Articles 1(e)(2), 28(e) and 33, and Annex VIII of the Staff Regulation of Officials;
- Articles 12(2)(d), 13, 28 (second paragraph), 82 (3)(d) and 83(2), 95 and 100 of Conditions of Employment of Other Servants (CEOS).

For Annual check-ups:

- Article 59(1) and (6) of the Staff Regulation of Officials;
- Articles 16 and 91 of CEOS.

For Reimbursements:

- Articles 28(e), 33 and 59(6), 72 of the Staff Regulations of Officials;
- Articles 13 and 16 of the CEOS;
- Article 48(1) of the CPVO Financial Regulation.

Legal Basis:

- Article 5(1)(a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

- CPVO staff members (Officials, Temporary and Contract Agents);
- Candidates for a CPVO vacancy.

10. When and how were data subjects informed

For Pre-employment visits: for candidates who successfully pass a competition for a position at CPVO, the Human Resource sector asks for a recent medical certificate. The Privacy Statement informing the data subjects about the processing is sent along with request to provide the recent medical certificate.

For Annual check-up: The Privacy Statement is shared along with the e-mail that is sent each year by the Human Resources staff member asking CPVO staff members to indicate whether they will undertake the annual medical checks with the contracting doctors of the CPVO-contracted medical centres. The Privacy Statement is also available to all CPVO staff members on the Intranet of CPVO, Sharepoint.

For Reimbursements: Upon responding by e-mail to the CPVO staff member's request for reimbursement, the Human Resources concerned staff member shares the Privacy Statement, which is also available to all CPVO staff members on the Intranet of CPVO, Sharepoint.

Information is given that if staff members decide to go to their own doctor, they will have to use the same relevant forms as for the contracting doctors of the CPVO and will be reimbursed, on request, in accordance with Article 59(6).

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected for the pre-employment and annual medical examinations are detailed in the Forms. During the examinations the following personal data may be collected:

- Name and surname, gender, nationality, place of birth, address, telephone numbers, profession and nature of the work (administrative or technical/research), family situation (optional), and sport activities (optional).

For Pre-employment visit and annual check-up:

- Medical history
- results of laboratory tests of blood[1]
- results of laboratory tests of urine[2]
- results of x-rays
- results of ECGs
- men over 50 are tested for prostate specific antigens (PSA)
- men over 45 are tested for stool samples

[1] The candidate's blood is tested for the following: complete blood count, thrombocytes, erythrocyte sedimentation rate (ESR), urea, serum, uric acid, creatinine, potassium, fasting blood sugar, gamma glutamyl transferable (if levels are elevated, also for transaminase SGOT and SGPT), total cholesterol, HDL, calculated LDL, triglyceride, total bilirubin, GGT, ASAT, ALAT protein electrophoresis, syphilis, haemoglobin, red blood cells, blood count, leukocyte, leukocystic formula.
[2] The candidates' urine is test for the following: albumin, sugar, microscopic examination, ph.

- testing for HIV is subject to the candidate's written consent and may be carried out only after the obligatory discussion of the subject
- results of a direct physical examination carried out by the Physician[3]
- psychological or psychiatric nature data ("psychisme")
- results of Ophthalmologist visit
- any other medical data results of complementary exams taken under CPVO request.

In addition, in the context of annual check-up, the following medical data must be processed:

- Chest X-ray test in case of (i) other examinations show its necessity or (ii) during the last annual visit before retirement
- electrocardiograms exam (carried out every two years for those who are more than 40 years old)
- gynaecological exam (including a physical examination and Pap smear) (for those who are more than 25 years old)
- mammography (for those who are more than 40 or if there is medical reason to do it)
- reproductive organs and rectal examinations (for men who are more than 45 years old)
- prostrate ultrasound examination (for those who are more than 50 or if there is a medical reason to do it)
- rectoscopy (carried out every two years for those who are more than 40 years old)
- rectoscopy (carried out every year for those with high blood pressure or with diabetes)
- syphilis test (carried out every five years only)

Regarding the reimbursement procedure:

- name and surname
- type of medical visit (if it is a general examination, an ophthalmology examination or a gynaecology examination, etc.)
- the total amount to be reimbursed.

The original documents ("feuilles de soins") can provide more detailed information. They can include date of service, name and address of the doctor, type of treatment/exam undertaken by the staff member.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit by *explicitly* specifying *the request* on the e-mail dpc@cpvo.europa.eu.

As for the medical files stored by the external processors, the staff members shall ask directly and individually the Cabinet medical d'Avrillé and the Cabinet d'Ophtalmologie d'Avrillé. For blood and urine tests, a copy of the results is sent directly by the laboratory to the staff member's home address.

13. Storage media of data:

Personal data in personal files are stored as hard copies in locked cupboards at the premises of the Human Resources sector. Electronic copies of the data are stored within the CPVO Internal database Docman.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data may be disclosed to internal and external recipients on a *need-to-know* basis:

Internal recipients (For reimbursement purposes):

- Employees of the Human Resources and Finance and Accounting sector of the CPVO;
- IT Administrators.

External recipients (for pre-employment and annual medical check-ups):

- External doctors appointed by the data subject;

[3] Weight, height, blood pressure, reflexes, status of tongue, tonsils, lungs, etc.

- "Medical service" of other Institutions in case of data subject transfer (under consent);

No personal data is transmitted to parties which are outside the recipients and the legal framework mentioned.

15. * Period of retention for the data:

According to the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, the information that a person is fit (in the context of both the pre-employment and the annual checks) is kept by the CPVO in the personal file only for a period of 3 calendar years will then be destroyed. Where a negative report (certificate or statement) is issued by the doctors (form received indicating that the person is not fit which will lead to non-employment of a successful candidate), the retention period is of 24 months.

In accordance with Article R1112-7 of the French Public Health Code (Code de la Santé Publique), the medical data stored by the contracted doctors must be kept for 20 years after the last consultation. For more information, please refer to the applicable law.

Regarding reimbursement:

According to the CPVO Financial Regulation (Article 48(1) FR), supporting documents for the accounting system and for the preparation of the accounts referred to in Article 87 of the CPVO Financial Regulation, the data related to reimbursement requests shall be kept for at least five years from the date on which the Administrative Council grants discharge for the budgetary year to which the documents relate.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

The certificate that is sent to the CPVO is classified in the personal files of data subjects. The hard copies that are kept in locked cupboards at the premises of the Human Resources sector are accessible only to authorised members of the Human Resources sector. The Human Resources staff members have signed an agreement with the CPVO on compliance with the confidentiality principle.

The written reimbursement request and its supporting documents will be stored in a specific file. This file is stored in a locked cupboard and only selected employees of the Human Resources sector shall have the access. The requests are also stored electronically in the internal database Docman, where access to such is password-secured. Only the Human Resources sector and the Financial sector have access to these documents on a *need-to-know* basis.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Publications of the CPVO

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 11

4. * Name and contact details of the Controller:

Head of Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit (Registry sector)

7. Description of the processing operation:

The CPVO, at least every two months, issues a publication on the Official Journal of the Community Plant Variety Office. It contains information concerning received application for CPVRs, termination proceedings regarding applications for CPVRs, proposal for variety denominations, changes in the identity of the applicant or procedural representative (if any), levy of executions, granted CPVRs including the species and variety denomination of the variety, name and address of the holder, of the breeder and of any procedural representative concerned, date on which the right is granted and will end (including reasons for termination) and when requested, any exclusive license agreement, including the name and the address of the person holding the exclusive right, when requested, any levy of execution. Where the holder of an initial variety and the breeder of a variety essentially derived from the initial variety so request, the identification of the varieties as initial and essentially derived including the variety denominations and the names of the parties concerned.

On the Official Journal of the CPVO, also S2/S3 publications are issued, providing applicants with further technical information as to the requirements for plant material species and according to Examination Offices entrusted to carry out DUS technical examination on behalf of the CPVO. Furthermore, once per year, the CPVO publishes an annual report, containing *inter alia* a list of valid CPVRs, their holders, dates of grant and expiry as well as approved variety denominations.

Personal data originates from applications received at the CPVO as well as further notices subject to publications by virtue of Article 89 of Regulation (EC) 2100/94. These data, once received, are automatically stored in PVR, internal database of the CPVO and extracted by the Register division within the Technical Unit in order to prepare the above-mentioned publications.

8. Purpose(s) of the processing and legal basis:

The purpose of the processing operation is to ensure compliance with Article 89 of Regulation (EC) 2100/94 and Article 87 of Regulation (EC) 874/2009, namely, requiring the Office to issue periodical

publications containing the information entered into the registers, for the sake of the public interest. As an EU Agency, the CPVO is bound to the general legal principles of openness and transparency.

Legal instruments:

- Article 89 of Regulation (EC) No 2100/94;
- Article 87 of Regulation (EC) No 874/2009;
- CPVO Decision of 19 February 2021 on the form of Registers, keeping of documents in electronic files, retention periods and publication of the Official Gazette.

Legal basis:

Articles 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

The categories of data involved are:

- Applicants for CPVR titles;
- CPVR holders;
- Procedural representatives of CPVR applicants;
- Breeders of varieties for which the CPVR title has been applied/protected under a CPVR title;
- Holders of essentially derived varieties;
- Licensees of contractual exploitation rights;
- Pledgees of CPVR applicants and holders.

10. When and how were data subjects informed:

The Privacy Statement is available on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data processed are the following:

- Name and Surname, and postal address of the CPVR applicant/holder;
- Name and Surname of the procedural representative;
- Name and Surname of the breeder;
- Name and Surname of the holder of an essentially derived variety
- Name and Surname of the holder of the contractual exploitation right;
- Name and Surname of the pledgee.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access and rectify his/her personal data in the cases foreseen by Articles 17 and 18 of Regulation 2018/1725, respectively, by submitting a written request to the data Controller, Head of Technical Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Data is stored on CPVO servers in France. Data is also stored in and made publicly available at the CPVO website as well as at in the website of the Publications Office of the European Union.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data is disclosed for public interest purposes to the general public through the CPVO website, as well as through the website of the Publications Office of the European Union.

15. * Period of retention for the data:

Once an electronic file has been generated that represents the true and complete copy of the file, based on paper documents or a similar medium (the "original"), the original shall be disposed of by the Office upon expiry of 3 years from the date of setting up of the electronic file. The electronic files, or back-up copies thereof, shall be kept indefinitely, unless a specific retention period for a certain type of files has been defined.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Data are made available to recipients in third countries or international organizations.

17. * Measures to ensure security of processing:

Upon receipt, data to be processed for the purposes of publications are automatically stored in "PVR", an internal database of the CPVO. Access to the latter is username- and password-protected and the information is stored securely as to safeguard the confidentiality of the data therein. For more information on this processing, please refer to Record No 74 Online Application System.

The software used to extract data from PVR and Contacts database, "lateX", is only accessible to the relevant staff members of the CPVO Register. The relevant data are extracted and subsequently published at the CPVO website.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Use of Social Media

2. * Last update of this record:

18/03/2021

3. Reference Number:

No 12

4. * Name and contact details of the Controller:

The President of the CPVO
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Presidency

7. Description of the processing operation:

The CPVO has adopted an external communication strategy aiming to promote the CPVO and the benefits of the EU-wide PVR System towards a larger public. The promotion of news, information and audio-visual contents is done on a frequent basis. The main social media adopted for communication are: Twitter, LinkedIn and YouTube (as a repository platform for video).

The Office posts on its official social media channels publications including video recordings, photos and screenshots (in case of video-conferencing/meetings) which may contain personal data. These may be taken during webinars, events and meetings with the Administrative Council, experts from Examination Offices, other EUIs and related bodies, QAS services, social events organised by the Staff Committee and further activities in the framework of international cooperation. Pictures may also be taken during oral hearings and shared through social media.

Furthermore, in order to keep abreast of the latest technical developments, business trends and policy debates in the field of Plant variety protection, the CPVO launched (January 2021) a series of webinars with technical experts. During the webinars, screenshots containing photos of the participants (external experts and staff members) may be taken, and are further shared on social media as LinkedIn and Twitter.

Previous consent of the data subjects is gathered before publishing the photos containing personal data on social media. Personal data may not be used for any other purposes.

8. * Purpose(s) of the processing and legal basis:

The CPVO, through its external communication strategy, aims at promoting the Community plant variety protection system in the EU and outside EU/EEA, informing stakeholders, enhancing dialogue and developing positive joint campaigns to highlight the benefits of PVR and new varieties for society, building support for the EU's policies and objectives by increasing the visibility of the CPVO activities and results, using plain language and thus bridging the gap between EUIs and citizens, sharing best practices and enhancing international cooperation in plant variety protection as well as enhancing the visibility of the PVR system as a sui generis IP vis-à-vis other IPRs and policy areas.

Legal Instruments:

- CPVO external communication & outreach strategy;
- CPVO social media policy (including Twitter guidelines);
- CPVO strategic plan 2017-2021.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (Processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority)

- As for the sharing of pictures on social media, Article 5.1(d) of the Regulation (EU) 2018/1725 (the data subject has given consent to the processing of his or her personal data for one or more specific purposes).

9. * Description of the category(ies) of data subject(s):

- CPVO staff members;
- Staff members of Examination Offices (EOs);
- Administrative Council members;
- Staff members belonging to institutions with which cooperation has been established;
- Staff members of EUIs;
- External experts participating in "The talk of the month" and further activities promoted by the CPVO;
- Parties to the proceedings before the Office and the Board of Appeal.

10. When and how were data subjects informed:

The privacy statement is available on the CPVO website under the Data Protection section. Consent of the data subject is gathered before any publication of photos of the data subject on social media.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Categories of data involved are the followings:

- Name, surname and of the data subject and link to the personal profile of the social media in question;
- Professional qualification of the data subject (sometimes);
- Photos or screenshots capturing faces of participants (CPVO staff members and external invitees) during webinars, events and meetings.

The controller ensures that no sensitive data is contained in the posts to be made publicly available.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, verify, block, rectify, object and erase his/her personal data in cases foreseen by Article 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725. The data subject has the right to withdraw the consent anytime. In all the cases, requests should be submitted to the CPVO data controller, President of the CPVO, at dpc@cpvo.europa.eu, by *explicitly* specifying the *request*.

13. Storage media of data:

Photos are stored on the relevant social media adopted for the specific communication. For more information regarding photos taken through meetings and events organised by the Office, please refer to Record No 45 Events and Meetings.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Access to the personal data is provided to CPVO Staff members responsible for carrying out the processing operation of preparing social media publications in accordance with the "need to know" principle and, in particular, to the following internal recipients:
- Presidency
- Selected staff members within the Procurement and logistic Service

External recipients:

- Wide general public through social media

15. * Period of retention for the data:

The posts published by the Office in its official social media channels including photos, screenshots and video recording and which may contain personal data are kept publicly available for an indefinite period of time unless the Office decides otherwise, or the data subject withdraws the consent.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Photos published on social media may be available to the wider general public.

17. * Measures to ensure security of processing:

All social media on Twitter and LinkedIn are public and can be consulted by anyone on these platforms. Videos uploaded on YouTube are either public or unlisted. Public YouTube videos can be retrieved by anyone visiting the CPVO YouTube channel or using the YouTube internal search engine. Unlisted YouTube videos cannot be retrieved via the YouTube search engine and are not displayed publicly in the CPVO YouTube channel. Only people having received the "link" of an unlisted video can watch. The CPVO is using unlisted videos for internal video messages.

For more information as regards security measures adopted when processing personal data for events and meetings, please refer to Record No 45.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Access to Personal Files by staff

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 13

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

Each staff member has a designated personal file, stored electronically and in paper. A staff member wishing to consult his/her electronic personal file, can do so by logging into the Office's internal database Docman, where his/her personal file is stored. The personal file is also accessible to CPVO staff members in SYSPER. A staff member wishing to consult his/her personal file stored in paper form, should submit a written request by email to Human Resources.

8. * Purpose(s) of the processing and legal basis:

The Human Resources sector processes the necessary personal data to establish a personal file for each CPVO staff member and to maintain it updated until the end of service of the staff member concerned. The European Commission also processes the necessary personal data in SYSPER.

Legal instruments:

- Article 26 of Staff Regulations;
- Article 11 of Conditions of Employment of Other Servants of the European Union (CEOS);
- CPVO Internal Procedure of 20 March 2021 to be followed by the CPVO Controllers in relation to rights exercised by data subjects in accordance with Regulation 2018/1725;
- SLA signed between the CPVO and European Commission (PayMaster Office, SYSPER 2).

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO staff members

10. * When and how were data subjects informed:

The Privacy Statement is made available on the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The personal file of a staff member contains:
- All documents concerning his/her administrative status and all the reports relating to his/her ability, efficiency and conduct;
- Any comment by the staff member concerned on such documents.

In particular, the personal file usually contains the following folders:
- Absences;
- Administrative acts;
- Career development;
- Certificates;
- Civil Status;
- Correspondence;
- Education and Training;
- Professional experience.

Regarding data contained in personal files in SYSPER, please refer to Record No 68 SYSPER.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725. In order to access personal file in paper form or rectify, block, object and erase his/her personal data kept in personal file, data subject must submit a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu by *explicitly specifying* the request. The CPVO has implemented the CPVO Internal Procedure of 20 March 2021 to be followed by the CPVO Controllers in relation to rights exercised by data subjects in accordance with Regulation 2018/1725.

13. * Storage media of data:

Electronic copies of personal files are stored in the internal database of the Office, "Docman", as well as in SYSPER 2. Physical personal files are stored in locked cupboards at the premises of the Human Resources sector.

14. * The recipients or categories of recipients to whom the data might be disclosed:

Personal data may be disclosed to the following recipients on a *need-to-know* basis:
- Human Resources sector;
- Concerned staff member;
- IT System Administrators (for the purpose of maintenance of the database).

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data contained in the personal file of a staff member will be destroyed after a period of 10 years from the date of the end of contract of the staff member. The end of contract can be due to a contract of limited duration, dismissal, resignation, retirement or death of the staff member.
Regarding the period of retention for data stored in SYSPER, please refer to Record No 68 SYSPER.

16. Proposed transfers of personal data to third countries or international organization and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organizations.

17. Measures to ensure security of processing:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate *need-to-know* base for the purpose of this processing operation. In this context, the physical personal files are locked in cupboards and can be accessed only by Human Resources sector. Access to electronic personal files within the database Docman is password-secured and can be accessed by concerned staff, HR and IT administrators on the *need-to-know* basis only.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

Regarding SYSPER, please refer to Record No 68 SYSPER.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Sales of Reports

2. * Last update of this record:

21/03/2021

3. Reference Number:

No 14

4. * Name and contact details of the Controller:

Head of the Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit

7. Description of the processing operation:

Within the framework of UPOV, and as approved by the Administrative Council of the CPVO, the CPVO can sell to national Plant Variety Rights (PVR) authorities DUS testing final reports on technical examinations of plant varieties (for which Community plant variety right (CPVR) protection has been applied) which have been conducted by the Examination Offices and have resulted in a positive report leading to the granting of the CPVR title of protection.

The concerned reports to be sold include both the positive final DUS report decision, leading to the granting of the CPVR title applied for (positive report), and the variety description, inclusive eventual photos of the concerned variety added by the Examination Office as annex to the variety description.

National PVR authorities can avail themselves of this possibility to avoid the high cost of technical examinations and to be able base their PVR-granting decisions on an existing final technical examination report. The exchange of report takes place against the payment of an administrative fee for the concerned report. The CPVO can invoice either the national authority or the breeder or his agent in the concerned country.

The requests from national authorities are either received by e-mail or by post. A form may be used to present the request for sales, based on the model "UPOV request for Examination results". The mailroom stores requests received at the CPVO reception in the internal document database called "Docman" (profile "Technical Matters", Theme "Report sales"). Upon receipt of the request, the concerned staff member in the Technical Unit registers the request in the internal database called "PVR". Automatic controls exist according to the file number recorded (type of examination, file status, financing regime). The agent prepares the reply adapted to the case (indicate the foreseen date of the final report in case it is not yet available, indicate the duration of testing and the submission period). If the final report has been issued, the fee is invoiced to the relevant party. Upon receipt of the payment the certified copies are sent out to the requesting national authority. For instance, if it is observed that an application for a CPVR has been withdrawn before the finalisation of the DUS test, a negative reply is sent to the requesting authority, as no examination of the variety is taking place and thus no DUS

report is going to be issued. If the CPVO took over the final report or if there is no CPVO application corresponding to the variety applied in another country (breeder reference or denomination and species do not match any CPVO application), a negative reply is sent to the requesting authority of this country.

8. * Purpose(s) of the processing and legal basis:

The purpose of the data processing is to enable the Sale by the CPVO of DUS Reports to PVR National Authorities.

Legal instruments:

- Article 27(3) Regulation (EC) No 874/2009;
- UPOV Document TGP/5 "Experience and Cooperation in DUS testing", including the forms "UPOV Request for Examination Results" and "UPOV Answer to the Request for Examination Results";
- Administrative Arrangements between the CPVO and the PVR National Authority on the Sale of the Report regarding the finance regime.

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Members of the PVR National Authority, the Applicant for the concerned national PVR title of protection, the Technical Experts in Examination Offices and staff members of Technically Qualified Bodies involved in DUS testing of varieties, the holder of the CPVR title for which protection has been granted and which DUS report is sold upon request by the PVR National Authority.

10. When and how were data subjects informed:

The Privacy Statement is made available on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are processed:

Upon receipt at the CPVO of the request of the PVR National Authority:
- Name of staff members requesting PVR National Authority;
- Breeder's reference of the variety subject to the application;
- Date of application for the national PVR title;
- Applicant for the PVR title (name, surname, and postal address);
- Details on the variety for which protection has been applied for (breeder's reference, variety denomination, botanical name of taxon, person who bred, or discovered and developed, the variety);
- Technical Questionnaire relating to the variety for which national PVR protection is applied (sometimes attached);
- If applicable, reference of prior applications for PVR protection for the variety concerned;
- Address where the Sales report invoice must be sent when the fee is not paid directly by the requesting authority.

Upon sending of the Report by the CPVO to the requesting PVR National Authority:

- Reference number of the concerned plant variety for which the DUS report has been carried out;
- DUS report and variety description, inclusive eventual pictures of the variety examined;
- Applicant/Holder details, date of application for the CPVR title;
- Name, postal address and contact details (phone, email, website) of Requesting PVR National Authority;
- Stamp of the CPVO;
- Name of the CPVO agent sending documents or certified copies to the relevant parties.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object): Data subjects has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of the Regulation (EC) No 2018/1725 by submitting a written request to the CPVO data controller, Head of the Technical Unit to the email address dpc@cpvo.europa.eu, by *explicitly* specifying the request by email.
13. Storage media of data: Paper copies of requests for the sale of reports and the replies are kept in the physical archives. All copies of requests for the sale of reports are kept in a digitalised form in the internal database Docman. Personal data are kept within the CPVO servers in France, according to security standards, with defined access and authorization.
14. The recipients or categories of recipients to whom the data might be disclosed: Staff members in the Technical Unit, as well as other CPVO staff members (as they have access to the internal database Docman), the Examination Offices, the concerned national PVR Authority.
15. * Period of retention for the data: In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place in such case: Data can be sent to national PVR authorities (within the framework of UPOV) outside the European Economic Area (EEA).
17. * Measures to ensure security of processing: The staff members in the Technical Unit that manage the sales of reports are bound by confidentiality clauses. Relevant and solid IT tool safeguards are in place to secure safe online communications in the exchange of emails between the CPVO and the Requesting PVR National Authorities. When the CPVO sends the final report requested to the Requesting PVR National Authority, this is done via certified secured email (certified copies are sent via the B2B secured platform of the CPVO).
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Annual Appraisal and Probationary and Management Probationary periods of the President and Vice-President of the CPVO

2. * Last update of this record:

08/04/2021

3. Reference Number:

No 15

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The processing operations address the annual appraisal and the probationary and management probationary periods of the President and Vice-President of the CPVO.

Regarding the annual appraisal:

Data are collected in a form (report). Once completed the report is sent to the reporting officers and a date for a formal dialogue is set. Both jobholder (the President or Vice-President) and reporting officers meet for a formal dialogue which covers the fulfilment of objectives and implementing of the Office's work programme, and a training plan addressing the objectives in relation to the agency annual work program and the personal development goals. Subsequently, the reporting officer draws up a draft career development report, which includes appraisals of efficiency, abilities and conduct in the service. The draft report is transmitted to the jobholder for the acceptance/refusal and the possibility to provide further comments.

If the jobholder refuses to accept the career development report, the reasoned refusal is transmitted to the Chairman of the Administrative Council who has 5 working days to deliver his/her opinion. After consultation with the Administrative Council, it confirms or amends the report. When the Chairman departs from the opinion of the Administrative Council, he/she must justify his/her decision. The report is then closed and communicated to the jobholder and to the Administrative Council.

Regarding the probationary period report:

Data are collected in a form (report). During the month which follows the first day of entry into service, the reporting officers meet the probationer in order to comment on his/her job description and to agree, in writing, on how the objectives and the performance level expected from the probationer will be assessed during the probationary period. At the latest one month before the expiry of the probationary period, a final report shall be drawn up on the efficiency of the probationer, on his/her competencies to

perform the duties pertaining to the post and on his/her conduct in service. The reporting officers fills in part of report before an official dialogue is held with the probationer. After the dialogue has been held, the reporting officers finalise the report and makes it available to the probationer, which in turn has a limited amount of time to accept/refuse and provide comments. In case of refusal, the procedure followed is the same outlined above for the annual appraisal.

Regarding the management of the probationary period:

Data are collected in a form (report). After the end of the management probationary period of 9 months, the reporting officers draw up a draft report. The probationer and the reporting officers hold a formal dialogue and at the latest 10 working days after this dialogue the reporting officers can either propose a positive appraisal of the management probationary period or propose its extension. After having been notified of the report in writing, the probationer has eight working days to comment on the report. A report is deemed to be accepted in case of absence of reaction of the probationer within the time foreseen.

8. * Purpose(s) of the processing and legal basis:

Data is processed to manage the procedures of the annual appraisal and probationary period of the President and Vice-President of the CPVO, including the drafting of reports concerning the evaluation of duties and management skills. The original of the respective reports are transmitted to the Human Resources Service at the end of the procedure and are conserved in the personal files of the President/Vice-President of the CPVO.

Legal instruments:

For the probationary and management probationary periods:
- Article 34, 44 and 46 of the Staff Regulations;
- Article 14 of the Conditions of Employment of Other Servants (CEOS);

For Annual Appraisal Reports:
- Article 43 of the Staff Regulations of Officials;
- Article 15(2) of the Conditions of Employment of Other Servants (CEOS).

Legal basis:

Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

President of the CPVO, Vice-President of the CPVO, Reporting Officer.

10. When and how were the data subjects informed:

The President of the CPVO and Vice-President of the CPVO are informed when signing the engagement contract of the 2 probationary reports to be drawn up during the first 6/9 months. They are also informed orally about the appraisal to be drawn up annually.

The Privacy Statement is also made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected:

- Name and Surname of Reporting Officers;
- Name and Surname, Category and Grade, Staff number of the President of the CPVO or Vice-President of the CPVO;
- Overall purpose, functions and duties, competencies and assessment of the President and Vice-President of the CPVO;
- Agreed objectives in order of priority, assessment criteria, objectives in relation to the agency's annual work program, personal development goals;
- Appraisals of efficiency, abilities and conduct in the service;
- In case the data subject requests to reconsider then the reasons are stated;

- Achievements of objectives;
- Signature of the reporting officers and signature of the President or Vice-President;
- Comments if the opinion of the Chairman of the Administrative Council departs from that of the Administrative Council.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request by email to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.* The right of rectification only applies to factual data processed within the evaluation procedure.

13. Storage media of data:

Data are collected in a form (annual appraisal report, probationary report or management probationary period report) which is kept in the personal file of the jobholder once signed. The reports containing personal data are stored as hard copies in locked cupboards at the premises of the Human Resources sector and/or as electronic copies in the internal database Docman.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal and external recipients have access to the data on a *need-to-know* basis:

Internal recipients:

- The President and Vice-President of the CPVO;
- IT System Administrator (for maintenance purposes)

External recipients:

- The Reporting Officers (two members of the Administrative Council);
- The Chairman of the Administrative Council.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data, including evaluation reports, will be destroyed after a period of 10 years.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organization.

17. * Measures to ensure security of processing:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

As regards security measures adopted for the electronic storage of personal files, Access to Docman is username- and password-protected and only the concerned recipients on a *need-to-know* basis have access to documents relevant to the procedure. In addition to the access right granted to selected recipients, both Docman may be accessed only by CPVO/users from the internal network (on premises) or through the remote VPN SSL.

Regarding physical copies of personal files including data, this is only accessible to authorised members of the Human Resources sector.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Cooperation with Examination Offices

2. * Last update of this record:

18/03/2021

3. Reference Number:

No 16

4. * Name and contact details of the Controller:

Head of the Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit

7. Description of the processing operation:

In accordance with Article 55 of Regulation (EU) No 2018/1725 and the procedure laid down in Article 15 of the Regulation (EC) 874/2009, the CPVO is required to arrange for technical examination relating to compliance with the conditions to grant CPVRs. Examinations must be carried out by competent national Examination Offices (EOs) entrusted with responsibility for technical examination of varieties of the species concerned by the Administrative Council (Entrustment procedure). The CPVO comes into agreements with national examination offices through designation agreements that are based on a valid entrustment decision by the Administrative Council of the CPVO.

Where an examination report is available (or the technical examination is in the process of being carried out) at an Examination Offices already entered into Designation Agreement with the CPVO, this latter may address a request for a Take-Over (TO) of the DUS report from the entrusted Examination Office. According to Article 27(4) of Regulation (EU) 874/2009, the TO procedure applies also to EOs located outside the EU, under the conditions that a cooperation agreement providing for this possibility exists and the technical examination complies with the conditions laid down in the cooperation agreement. The exchange of documents is done through the professional email of appointed staff members within the Technical Unit or the B2B exchange platform.

The above-mentioned cooperation activities entail transfer of data between the CPVO and national offices. However, some data may be already held by the receiving national offices (e.g. in case of TO Procedure, where the receiving office holds already personal information of the applicant, and only the personal information of the procedural representative is disclosed).

To be noted that the CPVO organizes meetings with experts from Examination Offices. For more information in this regard please refer to Record No 45 Events and Meetings.

8. * Purpose(s) of the processing and legal basis:

The purpose of the present processing is to carry out technical examination (DUS testing) as well as part of technical examinations on candidate varieties for the granting of Community Plant Variety Rights. In order to do so, documents containing personal data are exchanged between EOs and the CPVO.

Legal instruments:

- Articles 55, 56 and 57 of Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights;
- Articles 15 and 27 of the Regulation (EC) No 874/2009 of 17 September 2009;
- Entrustment requirements approved by the Administrative Council of 15 October 2015;
- Designation Agreements (DAs) between the CPVO and national Examination Offices (EOs);
- CPVO Take Over Procedure;
- Take Over Agreements.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);
- As regards the taking of pictures during meetings with Staff members of Examination Offices, please refer to Record No 45 Events and Meetings.

9. * Description of the category(ies) of data subject(s):

- Employees of the EOs involved in technical examination;
- Employees of the TQBs performing technical examinations on behalf of the EOs entrusted;
- Subcontractors of TQBs involved in technical examinations;
- CPVR/PVR applicants and breeders;
- CPVR/PVR applicants' representatives.

10. When and how were data subjects informed:

The Privacy Statement is available on the CPVO website, under the Data Protection section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Categories of data involved are the followings:

- Name, surname and email address, postal address, City, Country, telephone, nationality of the applicant/holder, if a natural person;
- Name, surname, e-mail address and postal address of the procedural representatives (if any);
- Name, surname, postal and email address of the breeder (if the breeder is not the applicant);
- Name, surname and email address of staff members of Examination Offices and staff members of Technically Qualified Bodies.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, verify, block, rectify, object and erase his/her personal data in cases foreseen by Article 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Technical Unit to the email address dpc@cpvo.europa.eu by *explicitly* specifying the request.

13. Storage media of data:

Personal data is stored in secure IT Systems according to the security standards of the CPVO. System and servers are password protected and require an authorised username and password to access. Depending on the document exchanged, personal data may be stored in both the Contact database and in Docman. Servers are located in France.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Access to the personal data is provided to authorised CPVO Staff members responsible for the processing on *a need-to-know* basis.

External recipients:

Data may be transferred to the following recipients:

- Bundesamt für Ernährungssicherheit, Austria
- Instituut voor Landbouw-en Visserijonderzoek ILVO eenheid Plant, Belgium
- Executive Agency for Variety Testing, Field Inspection and Seed Control, Bulgaria
- UKZUZ, Czech Republic
- Bundessortenamt, Germany
- Tystofte Foundation, Denmark
- University of Aarhus (Aarsalev), Denmark
- Agricultural Research Centre, Estonia
- OEVV, Spain
- Finnish Food Safety Authority, Finland
- GEVES, France
- Hellenic Ministry of Rural Development and Food, Greece
- Croatian Centre for Agricultural Food and Rural Affairs, Croatia
- NEHIB, Hungary
- Department of Agriculture Food and the Marine – Backweston Farm, Ireland
- CREA-VE, Italy
- CREA-DC, Italy
- CREA-OFA, Italy
- Servicio Nacional de Ispeccion y Certificacion de Semillas (SNICS), Mexico
- NAKTUINBOUW, Netherlands
- COBORU, Poland
- Direcao Direção Geral de Alimentação e Veterinária, Portugal
- Swedish Board of Agriculture, Sweden
- Central Controlling and Testing Institute in Agriculture (UKSUP), Slovakia
- Animal & Plant Health Agency (APHA), UK
- NIAB, UK
- Ministry of Agriculture and Rural Development, Agricultural Research Organisation (ARO), The Volcani Center, Israel
- The Intellectual Property Office of New Zealand, Ministry of Business, Innovation and Employment, New Zealand
- The Agriculture and Food Agency, Council of Agriculture, on the basis of an Administrative Arrangement;
- Oficina National de Semillas, Costa Rica
- Ministry of Agriculture, Forestry and Fisheries (MAFF), Japan
- The Council of Agriculture of the executive Yuan ROC Taipei, Taiwan, P.R. of China
- Plant Variety Protection Office, State Forestry Administration, P.R. of China
- State Service on right protection for plant varieties, Ukraine

In addition, also Technically Qualified Bodies in accordance with Article 53.6 of the Regulation (EC) No 2100/1994 and their sub-contractors are recipients to the extent that they are involved in technical examination.

15. * **Period of retention for the data:**

The retention period varies, depending on the nature of the documents.

16. * **Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:**

Data may be transferred to the following entities or international organisations:

- Ministry of Agriculture and Rural Development, Agricultural Research Organisation (ARO), The Volcani Center, Israel, based on a TO Agreement;
- The Intellectual Property Office of New Zealand, Ministry of Business, Innovation and Employment, on the basis of a TO Agreement;
- The Agriculture and Food Agency, Council of Agriculture, based on an Administrative Arrangement;
- Oficina National de Semillas, Costa Rica, on the basis of TO Agreement;
- SNICS, Mexico, on the basis of a TO Agreement;
- MAFF, Japan, on the basis of an Administrative Arrangement and a TO arrangement;
- The Council of Agriculture of the executive Yuan ROC Taipei, Taiwan, P.R. of China;
- Plant Variety Protection Office, State Forestry Administration, P.R. of China.

17. * **Measures to ensure security of processing:**

Personal data are stored in a secured IT System according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. The information is stored securely so as to safeguard confidentiality and privacy of the data therein.

Documents are exchanged through the professional email of appointed staff members within the Technical Unit or the B2B exchange platform. The email is username and password protected.

In accordance with the provisions laid down in Designation Agreements with Examination Offices, staff members of the Examination Offices taking part in a technical examination are bound by confidentiality in relation to any fact, document or information coming to their knowledge in the course of or in connection with the technical examination. The following applies also to Technically Qualified Bodies of Examination Offices and their sub-contractors.

18. * **For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.**

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Annual Appraisal of Officials, Temporary and Contract Agents

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 17

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The processing operations concerns the annual appraisal exercise, which begins on the 15th of January at the latest. Human Resources staff members begin by sending out the time table for the exercise and informs when the electronic platform Centurio is available for beginning the procedure of filling in the Appraisal form, named "Career Development Report" (CDR).

The Jobholder then completes sections 2, 3, 4 and 6 of the CDR form (Overall purpose of the job, Assessment of work and Personal Development Objectives, Self-Assessment against criteria and Certification procedure, if applicable Personal), reviews the current Forward Job and Development Plan (section 7) and drafts the Forward Job and Development Plan. Once completed and within the deadline set out in the relevant procedure, the form is transmitted to the Reporting Officer. The Reporting Officer gives some indication of the level of objectives he/she is looking for, and what areas should be covered, reviews and complete the form. In particular, he/she completes sections: 3 (Assessment of work and personal development objectives), 4 (Assessment against criteria), 5 (Overall Assessment), 6 (Suitability for the Certification Procedure) and 7 (Forward Job and Development Plan). He/she passes the form back to the Jobholder at least 48 hours before the CDR dialogue.

The Reporting Officer and the Jobholder hold a formal dialogue to discuss and agree Sections 1-6 as a minimum. The Jobholder's performance, efficiency and demonstrated ability to conduct the service are assessed. In particular:
- Jobholder's key responsibilities in the reporting period;
- jobholder's performance against objectives in the reporting period, and the evidence to be considered;
- jobholder's performance against the key criteria in the reporting period, and the evidence to be considered;
- any additional contribution the Jobholder has made to CPVO;
- the overall assessment of the Jobholder's performance during the reporting period;
- the objective(s) to be achieved against each key responsibility during the forthcoming year;
- the standards for assessing achievement of the objectives;

- the levels of competencies the Jobholder will have to demonstrate;
- the identification of the Jobholder's training needs in the development plan for the forthcoming year;
- suitability for the certification procedure (only for officials).

If the Jobholder does not act on the invitation to take part in the formal dialogue, without having been prevented from doing so by a justified absence, the Reporting Officer may immediately draw up an individual qualitative appraisal. Within ten working days of the formal dialogue, the Reporting Officer shall draw up an individual qualitative appraisal of the Jobholder's efficiency, ability and conduct in the service.

In the cases where the Jobholder's performance has been concluded to be unsatisfactory, the CDR shall be transmitted to the Countersigning Officer, in order to verify whether the appraisal procedure has been respected. If the performance is not deemed unsatisfactory, the Reporting Officer revises and signs the CDR to reflect the outcome of the dialogue and forwards it to the Jobholder for agreement and signature.

If the Jobholder does not refuse the CDR within the time limit set out in the relevant procedure, the CDR shall become final. The Jobholder sign the CDR and return it to the Reporting Officer. The Reporting Officer then transmits the CDR to the Human Resources Staff, who informs the President of the completion of the CDR for each staff member.

If the Jobholder does not agree with the CDR, the matter will be referred to the appeal assessor automatically.

Human Resources staff members store the CDR in the personnel file of the Jobholder. All changes to the Forward Job and Development Plans should be notified to HR, whenever they occur.

8. * Purpose(s) of the processing and legal basis:

The purpose of processing is to evaluate the jobholder's efficiency, abilities and conduct in the service and at identifying training needs, by drafting a report covering the period from 1 January to 31 December of the previous year for each staff member.

Legal instruments:

- Article 43 and 44 of the Staff Regulations;
- Article 15(2) and Article 87(3) of the CEOS,
- CPVO Decision on general provisions for implementing Article 87(1) of the Conditions of Employment of Other Servants of the European Union of 9 December 2015.
- CPVO Decision laying down general provisions for implementing Article 43 of the Staff Regulations and implementing the first paragraph of Article 44 of the Staff Regulations for officials and temporary staff, of 9 December 2015.

Legal basis:

Article 5.1 (a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Members of staff (officials, temporary agents and contract staff) who are engaged for a period of at least one year and who have worked for a continuous period of at least one month during the reporting period excluding staff members who were in their probationary period during the evaluated year.

This procedure does not apply to the President and the Vice-President of the CPVO, for which another decision and procedure applies.

10. When and how were data subjects informed:

The Privacy Statement is available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

The CPVO appraisal guide is also available to all staff members in the internal database Centurio and in the Vademecum on Sharepoint.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Data collected are:

- Personal information (name, current grade and personnel number);
- Job title;
- Performance (quality of work, productivity/effectiveness);
- Competences/ability (professional knowledge and know-how);
- Management and languages skills;
- Work objectives;
- Signature;
- Additional comments to the evaluation process by the data subject.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object or withdraw consent or the right to data portability):

The Data Subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpo@cpvo.europa.eu by explicitly specifying the request.

Important to note, the jobholder may always have access to his/her personal file in the internal database Docman and receive a copy of the appraisal report. Once finalised and signed, the final report cannot be modified.

13. Storage media of data:

The report is processed through the Centurio internal database, where the data are stored. Electronic copies of the report produced are stored in the personal file of the staff member concerned in Docman. Paper copies are stored in locked cupboards within the Human Resources' offices.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal and external recipients have access to the data on a *need-to-know* basis:

Internal recipients:

- Human Resources sector;
- The Reporting Officer;
- The President of the CPVO;
- Countersigning Officer (in case of unsatisfactory report);

External recipients:

- The Appeal Assessor (where the President acts as Reporting Officer, so that the Appeal Assessor should be idenfitied within the Administrative Council);
- The judicial authority in case of appeals;
- The Joint Committee (in case of unsatisfactory reports).

15. Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, Career Development Reports (CDRs) are destroyed after a period of 10 calendar years.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Data is not intended to be transferred to any third country or international organization.

17. * Measures to ensure security of processing: The organisational structure includes defined responsibilities for the various aspects of data protection. Access to Docman is username and password protected and only the concerned recipients on a need-to-know basis have access to documents relevant to the procedure. The same applies to files stored in the virtual servers of IT tool Centurio. In addition to the access right granted by the Human Resources sector to selected recipients, both Docman and Centurio may be accessed only by CPVO/users from the internal network (on premises) or through the remote VPN SSL. The only means to communicate data related to the report is through Centurio. Underlying reports cannot be read, copied or erased by anyone not authorised to do so. The internal database Centurio may be accessed by IT System Administrators for maintenance purposes. All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

International Cooperation

2. * Last update of this record:

31/01/2021

3. Reference number:

No 18

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processors:

- President of the CPVO
- Technical Unit
- IT Unit
- Legal service

External processors:

- Microsof
- Microsoft sub-processors
- A fix employee of Uplink

7. Description of the processing operation:

Within the framework of the CPVO's commitment to cooperate at international level with public national authorities in the field of plant variety protection, data is sent by the CPVO to different recipients in accordance with the objectives of the cooperation. Likewise, the Office receives relevant information in relation to the areas of cooperation as set out in Administrative Arrangements (AAs), Memorandum of Understanding (MoUs), and Protocols.

As regards training activities, conferences and workshops, data are processed by appointed CPVO staff members to organize and manage the event with the relevant party with which the bilateral cooperation has been established. The appointed staff member receives and gather personal data on the participants to the event, training activity, and/or workshop (both internal and external to the CPVO). In this context, the exchange of information is done through professional certified emails. For more information on processing in the context of events and meetings, please refer to Record No 45 Events and Meetings.

As regards communication exchanges on PVR applications and titles granted, the process varies depending on the receiving authority. The respective processing can be described as follows:

- Regarding bilateral cooperation with UPOV, the process is partially automated. The CPVO receives regularly notifications when new documents are uploaded on a UPOV server/database. This database is accessible to authorized staff members of the IT and Technical Unit, which may download the relevant information and upload it on the publicly available database of the CPVO, Variety Finder.
- Regarding bilateral cooperation with the European Patent Office (EPO), the CPVO receives regularly notifications when new EPO-related documents are made available on the CPVO's database. Likewise, the CPVO sends a monthly update to the EPO. The process is partially automated, as authorized CPVO staff members must manually retrieve the document once available in the database.
- Regarding EU Projects such as IP Key China, IP Key Latin America, and IP Key South East Asia, the CPVO, as European Partner, is involved within the framework of these projects in specific cooperation activities concerning plant variety rights, such as trainings.
- Regarding cooperation with Universities, the CPVO entered into agreements with several EU Universities, to educate IP specialists and to achieve greater awareness on plant variety rights.
- As for cooperation with national plant variety authorities, the exchange of information is, as general rule, carried out through emails between the CPVO staff member concerned, and the contact of the recipient belonging to the institution with which cooperation has been established.

Due to the outbreak of the Coronavirus COVID-19 pandemic, the Office has extended the use of "Microsoft Teams" ("MS Teams"), as part of Microsoft Office 365, to organize virtual meetings and videoconferences remotely with internal staff and external stakeholders, including those meetings taking place in the context of International Cooperation activities. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications between stakeholders and the Office.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is the facilitation and promotion of cooperation between the CPVO and relevant public authorities in the field of plant variety rights, both those inside and outside the EU, within the framework of the CPVO International Relations Strategy.

To this end, the CPVO organizes and takes part in conferences, courses, workshops and other meetings of mutual interest with the contracting parties. Amongst other, the CPVO shares technical knowledge on the management of plant variety rights, the testing of varieties, and on enforcement-related practices. The CPVO also provides trainings on the use of databases and other working tools to improve relevant data availability as well as optimizing reciprocal access to the information they have available.

Legal instruments:

- UPOV Convention;
- Article 27(3) of Regulation (EC) No 874/2009;
- Administrative Arrangements (AAs) signed with the concerned public authorities in the field of plant variety rights (or Intellectual Property rights) and other entities.

Legal Basis:

Art. 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. Description of the category(ies) of data subjects:

- CPVO staff members involved in international cooperation projects;
- Technical Experts (TEs) in Examination Offices and Technically Qualified Bodies involved in DUS testing of varieties for which they have been appointed;
- Staff members of entities with which cooperation has been established;

In exceptional circumstances, the data subjects may also be applicants for CPVR titles, holders of CPVRs, and procedural representatives.

10. When and how were the data subjects informed:

The Privacy Statement is made available on the CPVO website.

11. * Description of the category(ies) of data subject(s):

The categories of data processed are:

- Name and surname of CPVO Staff members involved in projects concerning international cooperation;
- Name, surname and email address of TEs involved in DUS testing;
- Name, surname and email address of staff members of entities with which cooperation has been established.

When processing personal data during the organisation of meetings via MS Teams, this personal data is processed in accordance with the Processing of personal data for the use of Microsoft Office 365 Desktop and online applications. Regarding MS Teams, as part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between the Office and its external users, such as messages, images, files, voicemails, calendar meetings, contacts, metadata used for the maintenance of the service provided.

In exceptional circumstances, particularly during workshops and trainings, pictures of the participants may be taken. For more information please refer to Record No 45 Events and Meetings. Likewise, exceptionally, for illustrative or educational purposes, for instance, in the course of trainings, data concerning an application for a CPVR or a CPVR title may be disclosed.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

Data subjects has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of the Regulation (EC) No 2018/1725 by submitting a written request to the CPVO data controller, Head of the Legal Service to the email address dpc@cpvo.europa.eu, by *explicitly* specifying *the request*.

13. Storage media of data:

Personal data are kept within the CPVO facilities in France, according to security standards, with defined authorization access.

When the CPVO, in the context of the cooperation established with specific public entities, receives relevant information subject to publication within the CPVO Variety Finder Database, it publishes the relevant information contained in the document forwarded and keeps a copy of the document within its own facilities. For more information, please refer to Record No 43 Contacts Database.

As for Microsoft, data are stored in Europe. However, additional data may be available to sub-processors outside the EU. Personal data are collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Access to documents containing personal data is provided to CPVO staff members on a *need-to-know* basis. Internal recipients vary in relation to the document at issue and the following: Presidency, Legal Service, Technical Unit, Administration Unit, QAS Service and IT Unit.

External recipients:

The category of data that may be disclosed varies in relation to the objective of the cooperation, in particular:

- The European Union Intellectual Property Office (EUIPO), in view of the MoU signed on 20 February 2015 (and extended) on bilateral cooperation. Data that might be transferred are: name, surname and address of trainees involved into the Pan European Seal programme, CPVO staff members, Temporary and Contract Agents in reserve lists and ID of contractors when they refer to a natural person. Furthermore, as the cooperation between the EUIPO and CPVO is aimed at the development of databases and IT projects, transfer of personal data may be necessary.

- International Union for the Protection of New Varieties (UPOV), in view of the MoU signed with the CPVO on 21 October 2004. Data subjects involved are PVR's applicants and CPVO staff members. Data disclosed are PVR applicant names registered in relation to denominations in databases. Moreover, the CPVO sends every year the CPVO staff names and trainees' names to the European Commission (DG SANTE) who then forwards them to the UPOV Office for the purpose of attending the UPOV distance learning courses and the UPOV Council meetings. Categories of data are: names, surnames, addresses, contact email and telephone of the data subjects.

- The European Patent Office (EPO), in view of the Administrative Arrangement on Bilateral Cooperation signed with the CPVO, on 11 February 2016. On a monthly basis, an update of CPVO data consisting of technical questionnaire and variety descriptions is sent to the EPO. Data subjects are CPVR applicants and procedural representatives. Categories of data are CPVR applicants' name, surname and address as well as name, surname and address of procedural representatives when appointed. The EPO is also recipient of personal data of trainees participating in the Pan European Seal Programme in light of Administrative Arrangement signed on 21 October 2016. Personal data involved are name and surname of the trainees.

- The Development Centre of Science and Technology, Ministry of Agriculture, P.R. of China in view of the AA 2017/0001 signed on 15 November 2017; also, STDC, Forest and Grassland Administration, P.R. China; data subjects are the signatory parties, activities coordinators and staff members involved; categories of data are only the name and surnames.

- The Ministry of Agriculture, Forestry and Fisheries (MAFF), in view of the MoU signed on 17 November 2006; data subjects are CPVR applicants and CPVO staff members. Personal data are names and surnames.

- The Organisation Africaine de la Proprieté Intellectuelle (OAPI), in view of the Protocol signed on 14 March 2002 and the EU funded programme TradeCom II – ACP Trade Capacity building programme; data subjects are the signatory parties, personal data involved are name and surname of the signatory parties as well as CPVO and OAPI staff members as well as experts involved from participating authorities, such as UPOV, GNIS, Naktuinbouw and GEVES.

- Agriculture and Food Agency, Council of Agriculture of the Executive Yuan, R.O.C. (Taiwan) China, in view of the AA signed on 27 April 2019 regarding PVRs protection of *phalaenopsis* and *doritaenopsis*; data subjects are CPVR applicants and Natkuinbouw's staff members (EO) involved in technical examination; categories of data are CPVR applicants' personal data and name and surname of staff members of the Examination Office involved in the technical examination.

- Munich Intellectual Property Law Centre (MIPLC), Germany, in view of the Collaboration Agreement between the MIPLC and the CPVO. Data subjects are staff members and students of Universities, staff members of the CPVO with the HR and Legal Service involved in selection procedure and/or co-curricular activities as establishment in the cooperation agreement.

Regarding MS Teams, the personal data is disclosed, under the need to know basis, to the following recipients:
- CPVO staff members and CPVO externals users included in the MS Team that is used for the exchange of information;
- Microsoft and its sub-contractors in order to provide maintenance, support or operation of the online service;

- IT Unit and an assistant from Uplink in order to provide the service and for maintenance purposes. The assistant from Uplink will have access to data upon IT administrator request and supervision only when replacing IT administrator on site.

15. * Period of retention for the data:

Data are retained as long as necessary in accordance with what has been established in the administrative arrangements.

As regards data processed under MS Teams, the data is retained for one year after the exchange activity is completed.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Data may be transferred to entities established in third countries (or international organisations) and entered into cooperation agreement with the CPVO. The transfer is usually limited to data necessary for the purposes of organising trainings and seminars (e.g.: booking related data). The following entities might receive personal data:

- European Patent Office (EPO);
- International Union for the Protection of New Varieties of Plants (UPOV);
- The Organisation Africaine de la Propriété Intellectuelle (OAPI);
- The Development Centre of Science and technology, Ministry of Agriculture, P.R. of China;
- The Council of Agriculture of the executive Yuan ROC Taipei, Taiwan, P.R. of China.

Regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by CPVO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise. If access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

17. * Measures to ensure security of processing:

<u>The CPVO:</u>

The CPVO stores data in secure IT system according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

As for training activities, conferences and workshops, access to the personal information contained in the relevant documents is restricted to specific staff members within the CPVO on a *need-to-know* basis.

<u>Microsoft:</u>

Microsoft implements appropriate technical and organisational measures to safeguard and protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them. Office 365 has been configured to preserve the confidentiality of the information exchanged by implementing encryption during all communications and in storage, and anonymous access is not authorized. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. Datacentres have physical and logical security monitoring measures. Finally, Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

PVR Case Law Database

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 19

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal Service

7. Description of the processing operation:

The PVR Case Law database is a CPVO online tool providing access for free to external users to the following documents:

- Judgements on plant variety rights' related matters taken by the Court of Justice of the European Union (CJEU) and by competent national courts of EU Member States;
- Legal decisions of the Board of Appeal of the CPVO;
- Legal decisions of the European Union Intellectual Property Office (EUIPO) (on EU Trade Marks applied for/registered in relation to products in Class 31 of the International Nice Classification);
- Legal decisions of the European Patent Office (EPO) (on matters interfering with plant variety rights).

The database provides the full text of the cited documents in their respective original language, as well as summaries thereof (in English). To this end, the appropriate translations are carried out by staff members in the CPVO Legal service. It must be noted in this regard that the documents supplied in the PVR Case Law database cannot be regarded as the official version of the judgements taken by jurisdictions within the EU/decisions taken by the cited deciding bodies. For access to the official decisions or judgments, the deciding body concerned must be consulted.

The PVR Case Law database offers different search criteria to assist the user in finding and retrieving the desired judgement/legal decision.

The described processing activity is ongoing, as the PVR Case Law database is being regularly updated with the latest relevant judgements and legal decisions in the domain of plant variety rights. External users may contribute to the content of the PVR Case Law database by asking questions or communicating additional information and cases to the CPVO, by addressing these to the following e-mail address of the CPVO: pvrcaselaw@cpvo.europa.eu.

8. * Purpose(s) of the processing and legal basis:

The CPVO maintains a public register with all the information regarding proceedings for PVRs for public interest. The case law database is maintained by the CPVO with the view to provide easy access to case laws/decisions relating to plant variety rights in one centralised repository.
These data are considered to be of public interest.

Legal instruments:

- Article 90 of Regulation (EC) 2100/94 on Community plant variety rights.

Legal basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Regarding decisions and judgements available in the PVR Case Law database, as well as in the summaries thereof:

- Parties to PVR-related legal proceedings;
- Procedural Representatives of the parties to the proceedings;
- Judges of the CJEU;
- Judges of the national courts competent for deciding on PVR-related matters;
- Appointed Members of the Board of Appeal of the CPVO and of the Boards of Appeal of the EUIPO;
- The President of the EPO
- Any other relevant Officials responsible for taking legal decisions;

Regarding email exchanges between any user and the CPVO concerning questions or the communication of additional information and/or cases to the CPVO in relation to the PVR Case Law database:

- External users sending the cited emails.

10. When and how were data subjects informed:

The data processed is regarded as data of public interest and in the public domain. The Privacy Statement will in any case be made available on the CPVO website dedicated page for PVR Case Law database.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Name and surname of parties to proceedings;
- Name and surname, and postal address of procedural representatives to parties to proceedings;
- Name and surname of other interveners in proceedings (e.g.: witness, experts);
- Name and surname, and signature, of the appointed judges/members of the CPVO or EUIPO Board of Appeal/President of the EPO/other officials in the concerned deciding body.
- Any other relevant data disclosed in the judgement or legal decision concerned.

It must be noted that the above data are made available in the PVR Case Law as initially published by the concerned court or deciding EU or European body, that is, the data was already in the public domain before being incorporated into the database.

Regarding particularly the exchange of emails between external users asking questions or communicating additional information and/or cases to the CPVO in relation to the PVR Case Law Database, further data may be shared with the Office, such as e-mail addresses and personal data on the contributors.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Legal service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request. In this regard, however, it must be recalled that the information made available in the PVR Case Law database is already in the public domain.

13. Storage media of data:

Electronic copies of the case law are stored in the PVR Case Law database, which can be accessed through the integrated search engine or on the CPVO website. Physical copies of the PVR case law Booklet are also made available to external users.

Regarding documents relating to preparatory activities preceding publications in the PVR Case Law database, such as the summaries by staff members of the CPVO Legal service for their subsequent upload into the PVR Case Law database, these may also be stored internally in the Intranet of the Office, Sharepoint.

14. The recipients or categories of recipients to whom the data might be disclosed:

The public at large.

15. * Period of retention for the data:

All personal data included in the PVR Case Law database are kept indefinitely for legal, historical and statistical purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The PVR Case Law database is accessible to any external user of internet.

17. * Measures to ensure security of processing:

The personal data available in the PVR Case Law database are stored in CPVO IT System according to security standards of the CPVO. External access to the database is username and password protected.

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate *need-to-know* for the purpose of this processing operation.

Access to Sharepoint (where related preparatory document are stored) is username and password protected and only the concerned recipients on a need-to-know basis have access to documents relevant to the procedure. In addition, Sharepoint may be accessed only by CPVO/users from the internal network (on premises) or through the remote VPN SSL.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Microsoft Office 365 Desktop and Online Applications

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 20

4. * Name and contact details of the Controller:

Head of IT Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of processor:

Internal processor:

IT Unit

External processor:

Microsoft Corporation (the service provider)
Microsoft sub-processors
A fix employee of Uplink (external service provider of the CPVO)

7. Description of the processing operation:

Office 365 is a cloud based package of applications provided to users with the aim to offer more flexibility and improve communications, collaborations, as well as the availability of resources. The processing operation will only cover, further to the software already in use on-premises (Word, Excel, PowerPoint, Outlook), Teams and One Drive.

The personal data is collected and stored in Microsoft Cloud servers with the purpose of providing the above-mentioned services.

8. * Purpose(s) of the processing and legal basis:

The purposes of processing data using Microsoft Office 365 Desktop and on-line applications is to provide professional services, including providing technical support, professional planning, advice, guidance, data migration deployment and solution/software development services, linked to the software tools Word, Excel, PowerPoint, Outlook, Teams and One Drive.

The processing is not intended to be used for any automated decision making, including profiling.

Legal Instruments:

- Framework Contract with DIGIT DI 07722;
- Article 42 of Commission Regulation (EC) 2100/94.

Legal Basis:

Article 5.1 (a) of the Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. When and how were the data subjects informed:

A privacy statement is made available on SharePoint and in the website to the data subjects and sent by email to all CPVO staff members and external providers with a CPVO user account.

All CPVO Staff members must be aware of the functionalities of the Microsoft Office 365 Package. To achieve this aim, the CPVO will ensure that all staff are given effective, regular, training, and the necessary administrative support to allow them to carry out their functions.

10. Description of the category(ies) of data subject(s):

CPVO staff members, external providers with a CPVO user account (a Windows account and a corporate email account) and subcontractors that use CPVO IS.

Regarding MS Teams, CPVO staff members and CPVO externals users included in the MS Team that is used for the exchange of information.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of personal data processed are the following:

- Personally identifying Information: username, name, surname, email, work telephone number, current function and preferred language;
- Electronic identifying information: IP address, cookies, connection data and access times;
- Movies, pictures, video and sound recordings;
- Metadata used for the maintenance of the service provided;
- Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21, 23 and 24 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The data is stored in Microsoft Cloud servers.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

IT Unit on a *need-to-know* basis.

External recipients:

Microsoft, as well as Microsoft's subcontractors included in the Online Services Subcontractor list and in the Microsoft Commercial Support Contractors list. The IT assistant from Uplink will have access to data upon IT administrator request and supervision only when replacing IT administrator on site.

15. * Period of retention for the data:

As regards Microsoft, data will be retained for as long as there is a contractual relation with the Office. Once a contract expires, information is retained for 90 days for the purposes of collection from the Office or possible renewal. After this period, information is deleted. As regards particularly the use of Microsoft Teams by the CPVO, data will be stored in Microsoft Teams for one year after the exchange activity is completed and then deleted after this period.

In the event of a disciplinary or criminal investigation, or formal appeal that involves information included in emails, all data held at the time of the formal appeal or investigation should be retained until the completion of the process.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Most customer data is kept in Europe, but additional data may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

In particular, regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by CPVO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

17. * Measures to ensure security of processing:

Microsoft 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 them. Microsoft Office 365 has been configured to preserve the confidentiality of the information you exchange by implementing encryption during all communications and in storage, and anonymous access is not authorized.

Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. Datacentres have physical and logical security monitoring measures. Finally, Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[1]

1. Name of processing:

Covid-19 Contact Tracing

2. * Last update of this record:

01/04/2021

3. Reference Number:

No 21

4. * Name and contact details of the Controller:

Head of Administration
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The CPVO has put in place a manual contact tracing system to trace whether the CPVO staff members have been exposed to Covid-19/have Covid-19 symptoms/have been tested Covid-19 positive. It must be noted that the Human Resources service does not get hold of nor process the specific medical details arising from the Covid-19 concerned infection/potential infection, as it is for the concerned CPVO staff member to contact on its own motion his/her medical practitioner. The CPVO only has data about the existence of a risk of exposure to Covid-19 or about the confirmation that a staff member is Covid-19 positive as reported by such staff member him/herself. The cited data is not transferred to any recipient outside the CPVO, including the French National competent Health Authorities.

The limited contact tracing system developed at CPVO primarily concern officials, temporary agents, and contract agents. They also apply mutatis mutandis to seconded national experts and, without prejudice of specific rules applicable to them, bluebook trainees. In what concerns external contractors (intra muros service providers, cleaning staff, security guards), specific provisions are communicated to them by responsible services within the framework of contracts entered into by the CPVO with firms (e.g.: "Plan de Prevention").

The measures taken by the CPVO in view of the Covid-19 pandemic outbreak, since the beginning of the outbreak and up until now, include several guidelines and procedures. A team led by the President of the CPVO was established to monitor the situation, provide guidance and inform staff about all decisions that were taken to preserve staff safety and maintain CPVO's Business Continuity Plan (BCP). Since March 2020, the BCP team has been constantly following the guidance of public authorities at EU, national and local levels.

The main process and data flow applicable to the manual contact tracing at the CPVO, as based on the current applicable CPVO De-Confinement Planning of 1 April 2021 are:

- The concerned staff member who has been confirmed as Covid-19 positive / presents any symptoms compatible with Covid-19 / has been in close contact and/or lives with a confirmed Covid-19 patient, must stay away from the CPVO premises and report the case to the Human Resources service.

- The Human Resources sector will indicate to the concerned staff member that he/she must remain at home and contact his/her medical practitioner. If the concerned staff member has been in the CPVO premises at the same time as another staff member (a maximum of two persons per floor is allowed), the Human Resources service will inform this staff member about the risk of exposure that has taken place and will ask him/her to self-quarantine for 14 days.

- The Human Resources sector will then launch a deep cleaning protocol of the CPVO premises. The Human Resources sector also collects and uses the data to establish a list of the staff with symptoms and/or tested positive of COVID-19, in order to be able to do the necessary follow-up and implementation of specific measures to secure the staff.

The CPVO has also put in place a system (presence calendars) to monitor presence of staff members/external contractors at the CPVO premises (three different buildings), namely, to ensure that a maximum number of persons are present at the same time for health security reasons (two persons per floor).

While carrying out the manual contact tracing, other processes are impacted, such as management of teleworking. For instance, the use of Microsoft Teams has been put in place and is now being used daily by the CPVO staff members to communicate with one another, as well as to carry out interviews in the context of recruitment procedures for CPVO vacancies and oral hearings with the CPVO Board of Appeal. MS Teams is a cloud-based application included as part of the Office 365 package.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing by the Human Resources sector is to implement the necessary mitigating measures for protecting the health and well-being of CPVO staff members and external contractors during the COVID-19 pandemic, as well as to conduct the necessary follow-up.

Legal Instruments:

- Article 1 (e)(2) of the Staff Regulations of Officials ("Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties");

- Articles L. 3131-15, L. 3131-16, and L. 3131-17 of the French Health Code (Code de la Santé Publique);

- French Décret n° 2021-248 du 4 mars 2021 modifiant les décrets n° 2020-1262 du 16 octobre 2020 et n° 2020-1310 du 29 octobre 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire.

Legal bases:

For checking occupancy rate in CPVO buildings and for Covid-19-related reporting by external contractors:

- 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 or in the exercise of official authority vested in the Union institution or body").

For contact tracing purposes, when involving health-related data:

- Article 10(2)(b) of Regulation (EU) 2018/1725 (the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject);

- Article 10(2)(h) of Regulation (EU) 2018/1725 (the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3).

9. * Description of the category(ies) of data subject(s):

CPVO staff members and external contractors.

10. When and how were data subjects informed:

CPVO staff members and some external contractors (security guards) were made aware of the processing operations by Human Resources Sector staff members via email. The Privacy Statement was also made available to CPVO staff members in the Intranet of the Office, under the Data Protection Officer section. A Covid-19 Internal Policy document was also published on Sharepoint, containing a description of the procedure to be followed preventing the spread of COVID-19 in the workplace and including also a notice and direct link to the cited Health crisis Record. Some other external contractors (cleaning staff) were informed on the need to report on Covid-19 contact/symptoms by means of a Prevention Plan agreed with the supplier company.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following categories of personal data are processed:

- Name and Surname of the staff member/external contractor concerned;
- Unit/Service in which the concerned staff member works;
- Building in which this person is located;
- COVID-19 symptoms from staff/external contractor and from anonymous household members – no indication of the name of such nor connection with the staff member/external contractor);
- Positive test results of COVID-19 (from staff member/external contractor and anonymous household members – no indication of the connection with the staff member/external contractor);
- Time of recovery/quarantine deemed necessary for resuming work.

No other data are sent to the CPVO.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The list of staff presenting symptoms and/or tested positive on COVID-19 is kept in an Excel file accessible only to authorised members in the Human Resources sector on a *need-to-know* basis. Access to the file is username and password-secured.

Regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by CPVO. However, it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

14. The recipients or categories of recipients to whom the data might be disclosed:

Only authorised staff members in the Human Resources sector (four persons) have access to the data.

15. * Period of retention for the data:

The list with the names of staff members presenting symptoms and/or tested positive of COVID-19 will be deleted once the above-described purposes cease to exist, account taken of the status of play of the health-risk circumstances arising from the Covid-19 pandemic outbreak. Email communications containing personal health data (namely, reporting on Covid-19 symptoms/exposure/positivity) will be deleted as soon as possible after receipt.

Regarding the use of Microsoft Teams by CPVO staff members, data will be stored in Microsoft Teams for one year after the exchange activity is completed. Further reviews of this period of retention may be made when deemed appropriate.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing

The list of staff presenting symptoms and/or tested positive on COVID-19 is kept in an Excel file accessible only to authorised members in the Human Resources sector on a *need-to-know* basis. Access to the file is username and password-secured and there are technical and organizational measures in place to ensure a highly secured IT system. The Human Resources staff members are bound by a duty of confidentiality in the exercise of their functions at the CPVO.

Regarding MS Teams, Microsoft implements appropriate technical and organisational measures to safeguard and protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them. Office 365 has been configured to preserve the confidentiality of the information exchanged by implementing encryption during all communications and in storage, and anonymous access is not authorized.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Organization and Recording of Oral Proceedings in Board of Appeal proceedings, including the Taking of Evidence (in-vivo and by videoconference)

2. * Last update of this record:

01/04/2021

3. Reference Number:

No 22

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Board of Appeal Registry

External processor:

Microsoft
Microsoft sub-processors
A fix employee of Uplink

7. Description of the processing operation:

In relation to appeal proceedings and the taking of evidence before the Board of Appeal, parties to proceedings are entitled to make oral statements. After the remittal of the case, the Chairman of the Board of Appeal shall summon the parties to the appeal proceedings to oral proceedings. The said communication is sent by email by the Registrar to the Board of Appeal.

In order to provide logistic support to the members of the Board of Appeal, the Registrar may share their personal data with hotels if accommodation arrangement are needed to participate in oral proceedings and the taking of evidence at the premises of the Office.

Due to the outbreak of the coronavirus COVID-19 pandemic, the Office has extended the use of 'Microsoft Teams' ('MS Teams'), as part of Microsoft Office 365, to organise virtual meetings and videoconferences remotely with internal staff and external stakeholders, including the Members of the Board of Appeal, the parties to proceedings and their procedural representatives attending oral proceedings and the procedures for the taking of evidence by and before the Board of Appeal.

MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and

file sharing. The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services. During oral proceedings before the Board of Appeal both in-vivo and by videoconference, the Registrar to the Board of Appeal will record the oral proceedings with the aim of drawing up the minutes of the oral proceedings. The parties to proceedings shall be provided with a copy of the minutes, and where appropriate, a translation thereof.

Photographs of oral proceedings may be taken during the hearing and published for internal or external communication purposes. At the beginning of the hearing, the Chairman will read a statement regarding the consent to the taking of photographs. The Chairman will also indicate that the hearing is recorded for the purpose of drawing up the minutes of the oral proceedings, as stated in the summons and that the parties to proceedings are not allowed to record the hearing themselves, either by video or sound recordings, when oral proceedings take place by videoconference using MS Teams.

8. * Purpose(s) of the processing and legal basis:

Personal data are processed for the management and condut of oral proceedings, the taking of evidence, coordinating any required follow-up activities, as well as for accountability and communication and transparency purposes. This may include registration of participants to the oral proceedings and the taking of evidence; logistic support before and during the event, minutes-taking and distribution of minutes, web-publication, and files sharing. Audio recordings of oral proceedings and the taking of evidence is carried out for the purpose of drafting the minutes. The data subjects will be informed by email in the invitation letter and confirmation of attendance by the Registrar to the Board of Appeal.

The purpose of taking of photographs either is external communication purposes (e.g.: promotion of the CPVO or social media), either for internal communication purposes (e.g.: the blog "Staff news" on SharePoint home page or historical archiving).

The processing of personal data is not intended to be used for any automated decision making, including profiling.

Legal Instruments:

- Articles 71(2) and 77 of Council Regulation (EC) No 2100/94 on Community plant variety rights;
- Articles 4, 50 of Commission Regulation (EC) No 874/2009 establishing implementing rules for the application of Council Regulation (EC) No 2100/94 as regards proceedings before the Community Plant Variety Office.

Legal Basis:

- Article 5.1(a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).
- Article 5.1 (d) of the Regulation (EU) 2018/1725 (the data subject has given explicit consent to the processing of those personal data for one or more specified purposes).

9. * Description of the category(ies) of data subject(s):

Party to proceedings, witnesses and/or experts, members of the Board of Appeal, staff of the CPVO, staff of the examination offices, interpreters if needed and the general public. Regarding MS Teams, CPVO staff members and any CPVO externals users including the Members of the Board of Appeal, the parties and their procedural representatives included in the MS Team that is used for the exchange of information.

10. When and how were data subjects informed:

Information to data subjects is provided in the Privacy Statement available in the email sent to summon them to theoral proceedings and the taking of evidence and explicit consent to the taking of photographs is asked in said email.

The Privacy Statement is also available in the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

During the processing activities (organization, recording, hearings and taking of pictures), the following data will be gathered:

- Username, name, surname, email, work telephone number, current function and language.
- Electronic identifying information: IP address, cookies, connection data and access times.
- Movies, pictures, video and sound recordings.
- Metadata used for the maintenance of the service provided.
- Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar)

- When processing personal data during the organisation of meetings via MS Teams, this personal data is processed in accordance with the Processing of personal data for the use of Microsoft Office 365 Desktop and online applications. Regarding MS Teams, as part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between the Office and its external users, such as messages, images, files, voicemails, recordings (if previously agreed), calendar meetings, contacts, metadata used for the maintenance of the service provided.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No. 2018/1725 by submitting a written request to the data controller, Head of Legal Service, by *explicitly* specifying *the request.*

13. Storage media of data:

Data is stored in Docman, Sharepoint, Outlook, and the Office secure files transfer Platform. Servers are located in France.

As for Microsoft, data is stored in Europe. However, additional data may be available to sub-processors outside the EU (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

All the recipients have access to the data processed on a *need-to-know basis*. They are the following: Parties to the proceedings, Members of the Board of Appeal, Registrar to the Board of Appeal, the general public present in the hearing and IT administrators have an access on the *need to know* basis.

Regarding the photographs, the general public will have access through the external publication channels of the Office (e.g. promotion of the CPVO and in Twitter and LinkedIn accounts). Staff members will have access through the internal channels(e.g. the blog "Staff News" on the internal network SharePoint's home page or historial archiving).

Regarding MS Teams, the personal data is disclosed, under the need to know basis, to the following recipients:
- CPVO staff members and CPVO externals users included in the MS Team that is used for the exchange of information;
- Microsoft and its sub-contractors in order to provide maintenance, support or operation of the online service;
- IT Unit and an assistant from Uplink in order to provide the service and for maintenance purposes. The assistant from Uplink will have access to data upon IT administrator request and supervision only when replacing IT administrator on site.

15. * Period of retention for the data:

- Docman: perpetuity;
- Office secure files transfer Platform: 60 days;
- Outlook: 4 years;
- Sharepoint: 10 years;
- Sound recordings will be retained until the minutes of the oral proceedings or taking of evidence have been signed;
- MS Teams: data will be stored in MS Teams for one year after the exchange activity is completed;
- Photographs retained for longer periods are only those related to hearings regarding on-going proceedings. In this case, the personal data will not be kept longer than 10 years. However, for photos published on social media, the personal data is retained until the data subject withdraw the consent. Please see Record No 12.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to any third country or international organizations.

As regards the use of Microsoft Office 365 and online applications, most customer data is kept in Europe, but additional data might be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

In particular, regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by CPVO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

17. * Measures to ensure security of processing:

CPVO:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

Personal data is stored in secure IT System according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. The information is stored securely so as to safeguard the confidentiality and privacy of the data therein.

The organisational structure includes defined responsibilities for the various aspects of data protection.

As for the e-emails sent in the course of the proceedings, the access is restricted to the e-mail addressee.

Microsoft:

Microsoft implements appropriate technical and organisational measures in order to safeguard and protect the personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them. Office 365 has been configured to preserve the confidentiality of the information exchanged by implementing encryption during all communications and in storage, and anonymous access is not authorized. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. Datacentres have physical and logical security monitoring measures. Finally, Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controllers declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Variety Finder User Account

2. * Last update of this record:

29/03/2021

3. Reference number:

No 23

4. * Name and contact details of the Controller:

Head of Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit

7. Description of the processing operation:

The Variety Finder database and search tool contains data on registered and proposed national and EU plant variety denominations (CPVRs and national Plant variety rights - National Lists and Commercial registers), Plant Patents, EU trade marks for Class 31 of the International Nice Classification system registered with the European Union Intellectual Property Office (EUIPO), Protected Designation of Origins, Protected Geographical Indications, and on other types of registers (i.e. OECD data). Variety Finder contains information on registers of more than 60 countries.

The Variety Finder search tool offers a number of criteria for users to conduct searches relating to the above described data. Searches in the database remain anonymous and users cannot be identified by CPVO staff members. Variety Finder also offers the possibility to test denominations for similarity between variety denominations in the framework of PVR or National Listing procedures in the EU, as well as similarity between variety denominations and EU trade marks. Details of the "Denomination Test" are recorded to allow users to retrieve previous tests.

Further, national PVR authorities as identified users have the possibility to ask for the CPVO advice as to the suitability of denominations. For more information, please refer to Record 31 Cooperation Service on Variety Denominations.

A natural or legal person wishing to consult the database is required to sign up to gain access. When signing up, the person is required to fill-in certain data in a form (name and surname; and contact details such as e-mail and postal addresses). Some data must be provided mandatorily, other data can be provided at the discretion of the user. The data, once received, is automatically stored within CPVO servers.

8. * Purpose(s) of the processing and legal basis:

The purpose of this processing is to allow users to obtain the relevant information from the database. It also allows the CPVO to monitor the use of the database, defining priorities for IT developments, to produce

statistics on the use of CPVO Variety finder, analysis and various reports based on Countries or Area (also outside EU) and type of organization using the database.

Regarding the production of statistics, the Office analyses data related to "Denomination Tests", the details of which are recorded to allow users to retrieve previous tests in the section "My tests".

The "Contact ID", a unique identifier created automatically in the internal database of the CPVO once a new user register a new account, is the data used for the production of statistics. This data, on its own, does not allow the identification of the user. Statistics are obtained through the use SQL Query, validated by the IT Unit and used by the Denomination team to fetch the data from the database. The internal software used to produce statistics is Tableau. For more information on Tableau, please refer to Record No 70 Tableau.

Legal instruments:

- Article 90 of Regulation (EC) 2100/94 on Community plant variety rights.

Legal Bases:

- Article 5.1 (a) of the Regulation (EU) 2018/1725 (the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. Description of the category(ies) of data subject(s):

Persons creating their account in Variety Finder.

10. When and how were data subjects informed:

The Privacy statement is accessible when registering user account on *Variety Finder* on the CPVO website.

11. Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data:

The following data are the ones collected in the phase of registration on Variety Finder:
- Login (username);
- Identification as a legal or natural person;
- Name and Surname;
- E-mail address;
- Address details (street/place, postal code, city, Country).

The following information, not mandatory, might be also gathered:
- Phone number;
- Fax number;
- Company name and website;
- Whether the new user had business with the CPVO.

12. Procedure to grant data subjects rights (right of access, to rectify, to block, to erase, to object)

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 19, 20, 21 and 23 of the Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data Controller, Head of Technical Unit, at dpc@cpvo.europa.eu by *explicitly* specifying the object of the request.

13. Storage media of data:

Personal data collected when signing in the Variety Finder database is stored in the Contacts Database of the CPVO. Servers are located within the CPVO premises.

14. The recipients or categories of recipients to whom the data may be disclosed:

Data may be disclosed to the Denomination Team and IT Unit for the update, functioning and maintenance purposes. As regards the production of statistics, only the ID Contact is disclosed and the data alone cannot be traced back to personal identifying information.

15. Period of retention for the data:

Personal data is retained during the whole duration of the use of the account by the data subject. Accounts where there is inactivity are automatically deleted. Likewise, where the user decides to exercise his/her right of erasure, the personal data are erased within fifteen days from the receipt of the request. The Contact ID however, may be stored for a longer period and can be traced back to personal identifying information only in case the user has another business/activity with the CPVO for which another purpose of processing applies (e.g.: the user is an applicant for a Community Plant Varity right).

Personal data provided by users who created an account and did not validate within few days are removed automatically from the internal database.

16. Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. Measures to ensure security of processing:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

For more information on data stored in the Contacts Database, please refer to Record No 43 Contacts Database. As to security measures adopted when producing statistics, please refer to Record No 70 Tableau.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

---

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Recruitment of Interim Agents

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 24

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processor:

Interim Agencies (currently, the Agency "Proman-Emploi")

7. Description of the processing operation:

The recruitment of interim agents is justified when there is an exceptional increase of work or special tasks have to be performed. In certain cases it is also justified for replacement (holidays, sick leave, maternity leave, etc.). To this end, the CPVO may enter into contracts with interim agencies. The current agency providing interim candidates to the Office is "Proman-Emploi" (website of the Interim Agency: https://www.proman-emploi.fr/).

Further to the decision of the Management Team that there is a need to recruit an interim agent, the Human Resources sector is responsible for preparing an informative notice on the new position, the tasks to be performed, the qualification required, the salary, and the period of time of the contract. The interim agency is requested to provide CV's corresponding to the identified needs.

A pre-selection of candidates will then be done by the Human Resources sector or the Head of Unit concerned. These candidates will be invited for an interview. Once the interviews have taken place, and a person has been selected, the interim agency is contacted and requested to draw up a contract. This contract is signed by the interim agency and the President of the CPVO.

The CPVO does not keep a personal file for the interim workers, nor remunerates them directly. The contract is with the interim agency, to which the CPVO pays the remuneration.

8. * Purpose(s) of the processing and legal basis:

The processing operation is necessary to hire agents during times of workload peaks, or of temporary and occasional staff shortages, or of need for the performance of special tasks.

Legal instruments:

- Directive 2008/104/EC of 19 November 2018 on temporary agency work;
- The French "Code de Travail", in particular the 1st chapter of the title V "Contrat the travail conclu avec une enterprise de travail temporaire", Articles L1251-1 to L1251-4 (a version of the document can be found on the website: www.legifrance.gouv.fr).

Legal Basis:

Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Candidates for interim agency posts in the CPVO.

10. When and how were data subjects informed:

When invited for the interviews, the Privacy Statement is sent to the candidates in advance. The Privacy Statement of the Interim Agency Proman-Emploi is available at: https://www.proman-emploi.fr/politique-confidentialite.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following personal data are processed for each candidate:
- Candidate reference number;
- Name and Surname;
- Title;
- Place and Date of birth;
- Nationality;
- ID card or passport;
- Contact details (E-mail address and phone number);
- Postal address;
- CV, including knowledge in languages, educational background, and professional experience, IT skills, and soft skills.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, the Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The data is stored in electronic files in the Internal database "Docman", and files in paper are locked in cupboards at the premises of the Human Resources sector.

Regarding the Interim Agency Proman-Emploi, data is stored in the servers of the agency.

14. The recipients or categories of recipients to whom the data might be disclosed:

Human Resources sector, the Head of Unit in which the interim agent is needed and the Interim Agency contracted by the CPVO (currently Proman-Emploi).

15. * Period of retention for the data:

In accordance with the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members, all

personal data submitted following recruitment procedures will be destroyed after a period of 24 months from the date of the decision of the Office appointing the successful candidate.

According to the Financial Regulation (Article 48(1) FR), supporting documents for the accounting system and for the preparation of the accounts referred to in Article 87 of the Financial Regulation shall be kept for at least five years from the date on which the Administrative Council grants discharge for the budgetary year to which the documents relate.

Regarding the Interim Agency Proman-Emploi, the candidates' data is retained for 24 months in the case of non-recruited candidates from the date of last contact with the candidate. Regarding recruited candidates, the data is retained during the whole duration of the recruitment and then for 24 months after the end of the contract concerned.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.
The same applies to the current Interim Agency Proman-Emploi.

17. * Measures to ensure security of processing:

The data is stored on paper in a file locked in cupboards at the premises of the Human Resources sector and accessible only to authorised staff members of this sector. Access to Docman is password-secured and access is only given to the Human Resources sector. IT Administrators can access on a *need-to-know* basis.

Regarding the Interim Agency Proman-Emploi, this agency puts in place technical and organizational measures to ensure the safety of the data stored.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[1]

1. Name of processing:

Retirement Procedure

2. * Last update of this record:

23/03/2021

3. Reference Number:

No 25

4. * Name and contact details of the Controller:

Head of Administration
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Internal processor:

Administration Unit (Human Resources sector)

External processors:

SYSPER 2 (European Commission)
PayMaster Office (PMO) (European Commission)

7. Description of the processing operation:

The processing is necessary to manage the retirement of a CPVO staff member and takes place under SYSPER (module CAR). SYSPER is a software created and managed by the European Commission, of which the CPVO makes use, which requires the processing of personal data in connection with the personal file of each staff member. For more information on the processing under SYSPER, please refer to Record No 68 SYSPER.

When a staff member leaves the CPVO due to retirement, the career's end and the decision date for the ending must be registered in SYSPER, where a reason for ending (retirement) must be introduced. The CPVO Human Resources sector prepares and transmits by e-mail the staff member's file to the Pensions section of the Paymaster Office (PMO.4).

The PMO keeps the data collected to correctly calculate and pay the retirement pensions.

The Human Resources sector sends the information to the PMO by e-mail. It is added to the personal file of the staff member and kept in a locked cupboard by the Human Resources sector and in the electronic filing system Docman.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is enabling the management procedure for the retirement of the CPVO staff member, including the granting and management of a retirement pension to be paid by the PMO.

Legal Instruments:

- Articles 77, 81 and 82 Staff Regulations of Officials;
- Article 4 of Annex IVa of the Staff Regulations of Officials;
- Articles 2, 3, 4, 5, 6, 8, 9, 9a, and 10 of Annex VIII of the Staff Regulations of Officials;
- Articles 20-28 of Annex XIII of Staff Regulations of Officials;
- Articles 39, 40, 109 and 110 of the Conditions of Employment of Other Servants (CEOS).

Legal Basis:

Article 5.1 (a) of the Regulation (EC) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Officials, Temporary and Contract Agents).

10. When and how were data subjects informed:

When the file of the concerned staff member needs to be disclosed to the PMO Pensions sector, the staff member is informed by the Human Resources sector in advance of this data processing operation. Further, the privacy statement is available at the intranet of the Office, Sharepoint, under the Data Protection Officer section. As regards processing operation in SYSPER, please refer to Record No 68 SYSPER.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected for processing the retirement pension is:

- Name and Surname;
- Personnel number;
- Date and Place of Birth;
- Nationality;
- Postal address;
- Personal e-mail address;
- Marital status;
- Spouse and dependent children-related data (Name and Surname, Date and Place of Birth, Nationality, Postal address, school enrolment in the case of children).

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting at dpc@cpvo.europa.eu a written request to the CPVO data controller, Head of Administration Unit, by *explicitly* specifying *the request.* The CPVO has put in place an Internal Procedure to be followed by the CPVO Controllers in relation to Rights exercised by data subjects in accordance with Regulation 2018/1725 dated 20 March 2021.

13. Storage media of data:

As for the external processor, the storage of data is on SYSPER servers of the European Commission, managed by DG DIGIT. According to the Annex 3 (Data protection) of the SLA between the CPVO and the Commission, data shall only be held in data centres located within the territory of the EU/EEA. Furthermore, the service provider may not change the location of data processing without the prior written authorisation of the client. Data is also stored at the PMO.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data is disclosed to internal and external recipients based on the *need-to-know* principle.

Internal recipients:

Human Resources sector

External recipients: SYSPER 2 (Commission) Paymaster Office (PMO)
15. * Period of retention for the data: According to the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, the data related to the management of the retirement procedure is kept by the CPVO in the personal file for a period of 10 years after the date of retirement of the staff member and will then be destroyed. The data in SYSPER will be kept for the whole duration of the payment of the pension to the retired staff member and, in case of death, to the beneficiaries of the survivor's pension.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: The data contained in the personal file of the data subject (sent to the PMO) is kept in locked cupboard in HR Service's office. The electronic copies are stored in Docman and accessible only to the members of the HR service by using username and password. As regards security measures adopted by the sub-processor, please refer to Record No 68 SYSPER.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Classification of Officials, Temporary and Contract Staff in Grade and Step

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 26

4. * Name and contact details of the Controller:

Head of Administration
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

When appointing permanent officials or engaging temporary or contract staff, the Appointing Authority in the CPVO may allow candidates an additional seniority of step in grade in order to take account of their specific professional experience, pursuant to Article 32 of the Staff Regulations. The classification exercise is conducted based on the following elements: (i) any duly certified professional experience connected with one of the agency's areas of activity (including the part-time experience) and according to the agency's needs; (ii) any periods of training and study; (iii) any compulsory military service or equivalent civilian service.

Candidates are responsible for providing the documents evidencing the official duration of their studies/training, the level of a degree or diploma/the equivalent level of a training period, the length of professional experience, professional activity during periods of training and further study.

8. * Purpose(s) of the processing and legal basis:

Determining the classification in grade and step upon appointment of the data subjects.

Legal Instruments:

- Articles 5, 29, 30, 31 and 32 of Staff Regulations;
- Commission Decision of 16 December 2013 laying down general implementing provisions concerning the criteria applicable to classification in step on appointment or engagement.

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

Permanent Officials, Temporary Agents and Contract Agents.

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects on the Intranet of the CPVO, Sharepoint, in the Data Protection Officer Section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

In order to determine the additional seniority of grade and step of the data subjects, the following data are processed:
- Name and surname;
- Period of education/training;
- Years and area(s) of professional experience;
- Period of compulsory military service or equivalent civilian service.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of the Regulation (EU) 2018/1725. In order to access personal file in paper form or rectify, block, object and erase his/her personal data kept in personal file, data subject must submit a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Electronic copies of personal files are stored in the internal database "Docman", and physical copies of personal files are stored in a cupboard at the premises of the Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Human Resources sector and IT administrators on the *need to know* basis.

15. * Time limits for erasure of the different categories of data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place in such case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Access to the internal database Docman is username and password-secured and can be accessed by the official in Human Resources sector. The physical files containing the data are locked in cupboards in the Human Resources premises. IT Administrators can access such documents on the *need to know* basis.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Assessment of the Ability to work in a Third Language

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 27

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Human Resources sector

External processor:

- European Personnel Selection Office (EPSO)
- SYSPER 2 (European Commission)
- If applicable, external language company

7. Description of the processing operation:

The Human Resources sector informs the concerned staff member of what is considered to be the first and second languages and invites them to choose a third language. The staff member provides information about the third language during the recruitment process. There are then two methods to demonstrate the necessary level in the third language: either by providing a copy of a diploma already obtained or by taking a test.

The CPVO does not assess the diplomas and certificates of staff members. It is always an assessment committee from EPSO who does that. After collecting the data, the training manager will send it to EPSO together with copies of the diplomas/certificates. EPSO will then assess the data and confirm to the CPVO the level of knowledge the staff member has on the third language.

If staff members choose to take a test recognized by EPSO, the HR sector (training manager) sends their identification information to an outside company, based in France, hired by CPVO for the purposes of organizing the test (contractor), although it remains possible for individuals to take a test through different organizations. If so, it will be up to them to enroll with the chosen organization and provide the relevant personal information. Then the CPVO training manager sends a copy of the diploma or certificate obtained to EPSO for record.

Another option is to take the test with EPSO. The HR sector (training manager) sends the name, the chosen language and the professional e-mail of the staff member to EPSO. EPSO proposes a test date

and the staff member registers him/herself to the test. The tests are done on-line. The result is sent to the staff member and to the training manager.

Once the ability to work on a third language of a concerned staff has been proved, the Human Resources sector will introduce the information in the staff member's personal file in Docman and in SYSPER.

In the case of a pending promotion/reclassification, the information is also disclosed to the Head of Unit and the AIPN to unblock the promotion/reclassification.

8. * Purpose(s) of the processing and legal basis:

Data are processed for the purpose of enabling EPSO (or the concerned external contractor) to assess the CPVO staff member's capacity to work in a third language before the first promotion after recruitment (Article 45(2) of Staff Regulations of Officials) and before the renewal of a contract for an indefinite period for type 3a contract staff in function group IV (Article 85(3) of the Conditions of Employment of Other Servants (CEOS)).

Legal Instruments:

- Article 45(2) of Staff Regulations of Officials;
- Article 7(2)(d) of Annex III to the Staff Regulations of Officials;
- Article 11 of the Annex XIII of the Staff Regulations of Officials;
- Article 85(3) of Conditions of Employment of Other Servants (CEOS);
- Commission Decision on joint rules laying down the procedure for implementing Article 45(2) of the Staff Regulations;
- Article 4 of the CPVO Decision of 17 June 2016 laying down general implementing provisions regarding Article 45 of the Staff Regulations (Decision of the President on Promotion Rules for Officials).

Legal Basis:

- Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Officials and Temporary Agents employed by CPVO, whether administrators or assistants and whatever their grade, who have not been promoted since they were recruited, and Contract Agents (type 3a contract staff in function group IV) who are subject to a renewal of their contract for an indefinite period.

10. When and how were data subjects informed:

The data subjects are informed by means of the dedicated Privacy Statement as well as of the Privacy Statement for SYSPER as uploaded in the intranet of the Office, Sharepoint, under the Data Protection Officer section. Where applicable, EPSO can also inform the data subjects with a Privacy Statement.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are processed:

- Personnel Reference Number;
- Name and Surname;
- Place of employment;
- First and second languages chosen for the recruitment competition;
- Choice of third language;
- Level of knowledge on the third language;
- Copies of certificates/diplomas.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The results of the language test (carried out with EPSO or with an external language company) sent to the training manager in the Human Resources sector is stored electronically in the internal database Docman as well as on paper in the dedicated personal file of the staff member concerned under locked cupboards at the premises of the Human Resources sector.

The data for first, second and third languages are also stored in SYSPER (PER data module).

14. The recipients or categories of recipients to whom the data might be disclosed:

Access to the personal data is provided to the CPVO, the EPSO Commission Staff responsible for carrying out this processing operation and authorised persons on a *need-to-know* basis.

Internal recipient:

The Human Resources sector, in particular, the training manager.

External recipients:

- EPSO;

- SYSPER 2 (please refer to Record No 68 SYSPER);

- Where applicable, also the external language company.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member. As regards the retention period for data held in SYSPER, please refer to Record No 68 SYSPER.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The data is not transferred to any third country or international organizations.

17. * Measures to ensure security of processing:

As regards SYSPER, the service provider ensures that employees authorised to process personal data, at any stage, have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality in accordance with the provisions of Article 16 of the SYSPER SLA.

Concerning personal data contained in electronic copies, this is stored in secured IT System according to the security standards of the CPVO. The servers are username and password-protected. The information is stored securely so as to safeguard the confidentiality and privacy of the data therein.

Regarding data in paper-based files, this is kept in the cupboards at the premises of the Human Resources sector and only accessible to selected members in it, in particular, to the training manager.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Unemployment Procedure

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 28

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Internal processor:

Administration Unit (Human Resources sector)

External processors:

- PayMaster Office (PMO) (European Commission)
- Pôle Emploi (French Unemployment Service)

7. Description of the processing operation:

When a staff member leaves the CPVO before retirement, without taking up employment elsewhere and stays in France, he/she has to enrol with the French Unemployment Service, Pôle Emploi. A file has to be completed and transmitted to that service. Pôle Emploi will use it to verify if the agent is entitled to unemployment allowance in France. If that is not the case, Pôle Emploi will issue a certificate that the agent should transmit to the CPVO Human Resources sector, so that the concerned staff member sends it by email to the PMO with a request for payment of the unemployment allowance. The PMO keeps the data collected in order to correctly calculate and pay the unemployment allowance. The Human Resources sector adds the data to the personal file of the staff member.

8. * Purpose(s) of the processing and legal basis:

The purpose of the Unemployment Procedure is to determine whether a staff member is eligible to receive the French unemployment allowance and, if not, receive the allowance of the PMO.

Legal Instruments:

Articles 28a and 96 of the Conditions of Employment of Other Servants (CEOS).

Legal Basis:

Processing is based on Article 5.1 (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. When and how were data subjects informed:

The Privacy Statement is available to all staff in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

The Human Resources sector provides all necessary data before the CPVO staff member's unemployment.

10. * Description of the category(ies) of data subject(s):

CPVO staff members (Temporary and Contract Agents).

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected for the processing of the unemployment allowance are:

- Name and Surname;
- Personnel number
- Place and date of birth;
- Nationality;
- Current and future postal address;
- Personal e-mail address;
- Entire career history;
- Salary statements.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Electronic copies of personal files are kept in the internal database Docman.

Physical copies are stored in the personal files of each staff member under locked cupboards at the premises of the Human Resources sector.

Regarding the external processors, PayMaster Office (PMO) and Pôle Emploi, these will also store data on behalf of the CPVO in their facilities and/or servers.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Human Resources sector
IT Administrators on a *need-to-know* basis

External recipients:

PayMaster Office (PMO) (European Commission)
Pôle Emploi

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data in the personal file will be destroyed after a period of 10 years after the end of the contract.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no proposed transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: The data sent to the PMO are kept in the personal file of the data subject. A copy of this file is also stored in a locked cupboard at the premises of the CPVO Human Resources sector, accessible only to authorised staff members of the Human Resources sector. Regarding the security of electronic copies of files, access to Docman is username- and password-protected and only authorised recipients on a *need-to-know* basis have access to documents relevant to the described procedure. The database Docman is only accessible via the internal network (on-premises) or via the remote VPN SSL. Human Resources staff members have also signed a confidentiality agreement.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Management of Missions

2. * Last update of this record:

26/03/2021

3. Reference Number:

No 29

4. * Name and contact details of the Controller:

Head of Administration Unit
Email address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
Email address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources Sector)

External processors:

Service providers

7. Description of the processing operation:

Participation on missions may be necessary within the framework of the Office's functions and strategic aims. Staff members willing to go on mission use the internal tool Centurio to launch the request. In parallel, staff members may request for travel and/or accommodation through the external service provider, providing details of date and time of meetings (and further information, where necessary). In the process of reservation, where Hotel ceiling are surpassed, approval by the Head of Unit of the purchase will be considered an approved derogation.

The hierarchical superior receives two requests to be validated via Centurio, namely the acceptance of the purchase of the ticket through the service provider and the acceptance of the request for mission. Once validated, the external service provider issues tickets and/or accommodation. Staff members may upload their personal or corporate credit card numbers to the online booking tool (service provider) to book certain low-cost flights and accommodation. The Human Resources sector receives the invoices from American Express and proceed with the validation just after the mission.

Where a mission requires a visa, the request may be made through the service provider. Upon creation of the mission request, the necessary folders are automatically created in an internal tool Docman and the supporting documentation is stored therein.

Upon return from the mission, the staff member must submit to the Human Resources sector all information regarding real costs incurred as well as PDF copies justifying these costs within three months. These information are stored in the internal database Centurio. The Human Resources sector proceeds with the calculation of the reimbursement to be made and introduces the statement of expenses and all

the supporting documents in Docman. The payment procedure is made in EPM via SIFI (an internal accounting IT tool) and staff member receives an automatic mail informing of the payment. The file is automatically archived in Docman.

8. * Purpose(s) of the processing and legal basis:

The purpose of the procedure is to allow the organization of missions of staff and the reimbursement of expenses incurred by the staff members while on mission in the interests of the Office. To ensure an effective management of the missions, the CPVO enters into agreements with service providers.

Legal instruments:

- Article 11-13a of Annex VII of the Staff Regulations of Officials;
- General implementing provisions of 2 July 2018 adopting the Guide to missions for officials and other servants of the CPVO.

Legal Basis:

Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All staff members having a statutory contract with the CPVO.

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section. The Privacy Statements of the service providers adopted is also made available in the Intranet of the Office Sharepoint.

Data subjects are also informed about the rules governing the missions through the publication on the intranet of the Office, Sharepoint, of several explanatory documents.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected are:

- Name and surname of the staff member;
- work telephone number;
- mission details, including place, purpose, duration, if combined with leave, hotel, number of nights, cost per night and other expenses;
- means of transportation used, costs, justification;
- amount to be paid;
- signatures from the staff member, and hierarchical superior;
- credit card number (Type, Number and Expiration date).

As regards the online booking tool and/or further companies used by the CPVO to provide the service, the following data are also processed:

- Login details (username and password);
- Date of Birth, Sex, Mobile phone, Emergency contact Number, Number and expiration date of Passports or Identity card, Country of Citizenship;
- Preferred Language and currency;
- Smoking preference;
- Various fidelity cards datas (e.g.,Thalys, Sncf, fight, etc.);
- connection data (e.g.: IP ddress).

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a

written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

As regards the relevant documentation to be filled by the staff member willing to go on mission, electronic copies of the documents are stored in the internal CPVO IT tools, Docman and Centurio. The servers located within the premises of the CPVO.

As regards the external subprocessors, data are processed into the online booking tools. Data are stored within the EU. However, additional data may be available to sub-processors with purpose of providing the service (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Data may be disclosed to the following recipients on a *a need-to-known* basis:

Internal recipients:

- Human Resources sector;
- Head of Unit;
- The Authorising Officer;
- The relevant staff member responsible for arranging missions (one designated staff member in each Unit/service);
- Accounting and Finance sector;
- IT System Administrator.

External recipients:

- American Express Global Business Travel (GBT) and its sub-processors;
- UVET France and its sub-processors;
- further service providers.

15. * Period of retention for the data:

In accordance with Article 42(5) of the CPVO Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate.

As regards external providers, the retention period for the data processed by UVET is set at 3 years after which data are deleted. Other service providers keep the personal data as long as necessary to provide the service and/or products, fulfil transactions requested as well as other essential purposes as compliance with a legal obligation.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Data is not intended to be transferred to third countries or international organizations. However, as regards the external processor American Express Online Booking Neo, data may be disclosed to third parties for the purpose of providing the service. Transfers of personal data are governed by Standard Contractual Clauses approved by the Commission as well as Binding Corporate Rules.

17. * Measures to ensure security of processing:

As regards regards electronic storage, both Docman and Centurio may be accessed only by CPVO/users from the internal network (on premises) or through the remote VPN SSL. Access to the specif documents is further secured by access rights granted by the Human Resources sector to selected recipients on a *need-to-know* basis.

All persons dealing with personal data in the context of IT Systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

As regards external contractors, the Controller verified that the external providers put in place all the necessary precautionary measures preserve the security of processing. The Controller monitors further implementation of security and organizational measures adopted by the external provider. The service providers ensure that employees authorised to process personal data, have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[1]

1. Name of processing:

Invalidity Procedure

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 30

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Internal processors:

Administration Unit (Human Resources sector)

External processors:

PayMaster Office (PMO) (European Commission)
Invalidity Committee (three Doctors)

7. Description of the processing operation:

In accordance with Article 53 of the Staff Regulations of Officials, a CPVO staff member who is recognised by the Invalidity Committee (three Doctors) as having a permanent incapacity to perform his/her duties, shall be automatically retired pursuant to Article 78 of the same regulations.

For this reason, the Invalidity Committee is set up, consisting of three doctors: the first appointed by the Office, the second appointed by the staff member concerned, the third appointed by common agreement between the first two doctors. The proceedings of the Invalidity Committee are confidential and remain in the medical file with the Medical Service of the Commission.

The Invalidity Committee takes a decision on the link between the staff member's incapacity for work and one or more of the four causes referred to in Article 78 of the Staff Regulations of Officials.

Once the proceedings are completed, the Invalidity Committee's conclusions are forwarded to the Administration Unit and the staff member concerned. The Invalidity Committee's conclusions do not contain any medical information. No medical information is disclosed in this document.

The medical considerations underpinning the Invalidity Committee's conclusions are separate from the conclusions forwarded to the Administration Unit and are set out in a detailed summary report, usually drafted by the third doctor. This summary medical report is annexed to the staff member's medical file.

The data needed to justify the right to invalidity allowance is prepared by the Human Resources sector according to the data available in the personal file, then validated and signed by the staff member

concerned. The forms containing the data is sent to the PMO Pension/Invalidity Service. The PMO then process the data in order to correctly calculate, and pay, the invalidity allowance.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing operation is to obtain from the Invalidity Committee a conclusion as to whether the Official, Temporary Agent or Contract Agent concerned should be granted invalidity.

Legal Instruments:

- Articles 53, 59 and 78, 81 and 82 of the Staff Regulations of Officials;
- Articles 13 and 14 of Annex VIII of Staff Regulations of Officials;
- Article 24(1) of Annex XIII of Staff Regulations of Officials;
- Articles 31, 33, 99, 101 and 102 of Conditions of Employment of Other Servants (CEOS).

Legal Basis:

Processing is based on Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Officials, Temporary Agents and Contract Agents).

10. When and how were data subjects informed:

The Privacy Statement is available to all CPVO staff members in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

In any case, where a staff member wishes to initiate an invalidity procedure, the Human Resources sector will provide him/her with all necessary information.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected for opening the invalidity procedure are:

- Name and Surname;
- Personnel number.

The data collected for producing the conclusion of the Invalidity Committee are:

- Medical file containing examination results of determined examinations by the Invalidity Committee.

The data collected for processing the invalidity allowance are:

- Name and Surname;
- Personnel number;
- Date and Place of birth;
- Nationality;
- Place of origin;
- Current and future postal address;
- Personal e-mail address;
- Marital status
- Entire career history
- Last salary statement
- Remaining leave entitlement
- Birth certificate of dependent child(ren)(if any)
- Declaration of intention of gainful employment
- Spouse's related information (Name and Surname; Date and Place of birth; Nationality; Postal address; Professional activity; Employer (if applicable); Proof of the spouse's annual taxable income (if gainfully employed).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Electronic copies of personal files are kept in the internal database Docman.

Physical copies are stored in the personal files of each staff member under locked cupboards at the premises of the Human Resources sector.

Regarding the external processor, PayMaster Office (PMO), this will also store data on behalf of the CPVO in their facilities and/or servers.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Human Resources sector (all data mentioned in point 11, except medical data underpinning the conclusion).

External recipients:

PayMaster Office (PMO) (European Commission) (all data mentioned in point 11, except medical data underpinning the conclusion).

Invalidity Committee (all data mentioned in point 11, except the data for processing the invalidity allowance). The Invalidity Committee may consult outside experts.

15. * Period of retention for the data:

The Invalidity Committee might review (depending on the grade of invalidity) the invalidity status every two years. If after that review, the staff member is considered apt to go back to work, the initial decision of the Committee will be destroyed. If, on the contrary, the staff member is still considered invalid, the initial decision and the new decision(s) of the Committee are kept in the file.

In that case, in accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data in the personal file of the staff member concerned will be destroyed after a period of 10 years after the end of the contract.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations outside the recipients and the legal framework.

17. * Measures to ensure security of processing:

The conclusion of the Invalidity Committee and the data sent to the PMO are kept in the personal file of the data subject. is kept in the personal file of the data subject. The physical file is stored in a locked cupboard at the premises of the Human Resources sector, accessible only to authorised staff members of the Human Resources sector on a *need-to-know* basis.

Regarding the internal database Docman, where digital copies of personal files are stored, is username and password-secured. The database Docman is only accessible via the internal network (on-premises) or via the remote VPN SSL.

All concerned recipients of data are under sworn oath of confidentiality.

18.	*** For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.**

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Cooperation Service on Variety Denominations

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 31

4. * Name and contact details of the Controller:

Head of Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit

7. Description of the processing operation:

Before accepting a variety denomination at national level, EU national authorities, as well as Norway and Switzerland (hereinafter, "national authority") have the possibility to ask for CPVO advice as to the suitability of denominations through the "Denominations tests" section of the "Variety Finder" database.

In addition to the standard options offered in the denomination test area, national authorities have access to a tick box "Request for CPVO expert advice", which allows them to ask the CPVO for analysis based on the result of the test they have performed.

CPVO deals with the requests for advice using the internal software "Denomanager". CPVO has access to the test results performed by the users in order to provide this advice.

The section "Your tests" in Variety Finder gives national authorities an overview of the tests they have performed. It allows them to follow the status of their requests for analysis and gives them access to the content of the CPVO analysis, to which the national authority has an option to reply, if needed.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is for the CPVO to assist national authorities in assessing the suitability of variety denominations, with a view to harmonise the interpretation and application of Article 63 of Council Regulation 2100/94 on Community plant variety rights.

Legal instruments:

- Article 63 of Council Regulation 2100/94 on Community plant variety rights;
- Commission Implementing Regulation (EU) 2021/384 of 3 March 2021 on the suitability of the denominations of varieties of agricultural plant species and vegetable species and repealing Regulation (EC) No 637/2009 (Text with EEA relevance);
- CPVO Guidelines on Plant Variety Denominations (version of 2018).

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Representatives of national authorities of EU Member States, Norway and Switzerland.

10. When and how were data subjects informed:

When requesting for the advice, the data subject can consult the Privacy Statement on "Variety Finder" on the first (*Welcome)* page.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are provided, when asking for advice:

- Name and Surname of the data subject, representative of the national authority;
- Name of the national authority;
- Country of the national authority;
- Date and time of request.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of the Technical Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the object of the request.*

13. Storage media of data:

The data related to the tests performed by the national authorities, whether they have been the subject of a request for advice or not, are stored in "Denomanager".

In addition, name, surname of the data subject, as well as country of the national authority displayed in both Variety Finder and Denomanager are stored in the "Contacts Database". The list of requests for advice made by a single authority is only available to the authority in question and the CPVO.

14. The recipients or categories of recipients to whom the data might be disclosed:

The Technical Unit staff members have access to the received requests. Only registered users of "Variety Finder" can access the provided advice by CPVO along with the request, submitted by the national authority.

15. * Period of retention for the data:

Advices provided by the Office, as registered, are not intended to be deleted, since they serve the ongoing purpose of improving the performance of national authorities and CPVO. The name and surname of the data subject requesting the advice are deleted after 5 years from submitting the request for advice.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Access to "Variety Finder" and "Denomanager" is password-secured. Access to Denomanager is given only to authorised staff members of the Technical Unit. IT administrators can access on a *need-to-know* basis. For more information on Variety Finder, please refer to Record 23 Variety Finder.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

E-signature Document Signing

2. * Last update of this record:

04/02/2021

3. Reference Number:

No 32

4. * **Name and contact details of the Controller:**

Head of Administration Unit
E-mail: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit

External processor:

DocuSign (https://www.docusign.com/) and its sub-processors

7. Description of the processing operation:

The CPVO avails itself of the tool "DocuSign" for signing documents electronically. This electronic signature is used, for instance, to sign designation agreements, R&D agreements, decisions of the Administrative Council of the CPVO. Documents to be signed with e-signature are uploaded into the DocuSign platform by the concerned CPVO staff member responsible for the document to be signed. In this platform, the names and email addresses of the signers must be indicated. By signing with e-signature, the concerned document is encrypted and a unique hash created.

The saved signature can be applied to PDFs, word processing documents and images. The signed document is sent to cloud storage for review. The CPVO staff member who used Dosusign also receives an email notification and copy of the document electronically signed.

The present record only covers the data linked with signing and storing a document. It does not cover the content of the documents themselves.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is enabling the electronic signature of documents.

Legal instruments:

- Articles 30, 35 and 42 (2) (a) of Council Regulation (EC) No 2100/94 on Community plant variety rights;
- CPVO Decision of 15 April 2016 on Use of electronic signatures.

Legal Basis:

Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

CPVO staff members, Chair of the Administrative Council, staff from external national Examination Offices in charge of technical examinations upon CPVO's request, and other parties to which documents to be signed are sent via the platform DocuSign.

10. When and how were the data subjects informed:

A privacy statement is available on the Intranet Sharepoint under the DPO section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

In addition to the content of the documents to be signed (all of which are governed by separate data processing privacy statements and records), the following information is collected as part of the process:

- Last Name, First Name;
- Date signed;
- E-mail address;
- Place and time signed;
- Electronic Signature;
- Phone number.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

CPVO:

All signed documents are stored within CPVO's online facilities (Sharepoint, Docman and CPVO servers) subject to strict rules of confidentiality.

DocuSign:

All documents are stored online for 90 days and can be downloaded and printed as needed by the persons involved in the workflow (sender/signer). Docusign adopts multiple datacenters for storage purposes, at regional level in the EU. Redundant copies of eDocuments may be stored in every data centre within the particular region to which a customer's account is assigned. In particular, data processed on behalf of the CPVO are shared with data centres in the EU (Frankfurt, Paris, and Amsterdam). By doing so, DocuSign assures performance, availability and business continuity of the e-signature service. All data centres belongs to Equinix, US company.

14. The recipients or categories of recipients to whom the data might be disclosed:

The data is disclosed to the signer, the sender and others put in copy of the signed document.

Data is also disclosed to DocuSign and to the datacenters used by DocuSign for storage purposes. Data centres are located in Germany, France and The Netherlands. Data centres in the EU belongs to Equinix.

Data is also disclosed to DocuSign affiliates in the EU/EEA, namely:

- DocuSign International (EMEA) Limited UK;
- Contract analytics Developmnet Sweden AB;

- DocuSign France SAS;
- DocuSign Germany GmbH.

In order to facilitate a "broad global access" user experience and to provide infrastructure services of DocuSign eSignature in the applicable country location, data might be shared between regions. In particular data may be shared with the following companies in the following locations: Cyxtera, in Tukwila, WA, and Chicago, IL, as well as SunGard, Richardson, TX, all based in the US. Data may be also shared with Microsoft Azure, data centres in Sidney and Melbourne, Australia, as well as in Toronto and Quebec, Canada. (please see list under point 16).

Data might be also transferred to Fusion BPO, Philippine and Sykes Enterprises Inc., in Philippines, Costa Rica and Egypt (please see list under point 16) in order to provide customers with the necessary support.

15. Period of retention for the data:

CPVO:

The normal administrative retention period for signed documents are 10 years, unless they are classified as having historical value and then, there is no retention period applicable.

DocuSign:

The retention period can be defined by the Administrator for DocuSign. This is set at 90 days after which documents sent to a queue to be deleted. The queue lasts 14 days, after which the documents within the envelopes are permanently deleted. All field data and any API attachments are also deleted.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

Data might be transferred by DocuSign to sub-processors outside the EU/EEA. In particular, DocuSign uses the following sub-processors outside the EU/EEA:

For Infrastructural sub-processors (all private entities):

Cyxtera – US
Microsoft Azure – Australia
SunGard – US

For DocuSign affiliates outside the EU:

ARX Inc. – US
Comprova.com Informatica Ltda – Brasil
DocuSign Acquisition Ltd – Israel
DocuSign Brasil Participações Ltda – Brasil
DocuSign Brazil, LLC, – Brasil
DocuSign Canada Ltd. – Canada
DocuSign International (Asia-Pacific) Private Limited – Dublin, UK
DocuSign International, Inc.- US
DocuSign Israel Ltd – Israel
DocuSign UK limited – UK

For customer success suppliers:

Fusion BPO – Philippine
Sykes Enterprises Inc – Costa Rica, Philippines, Egypt

Transfers to DocuSign affiliates are governed by BCRs, whereas transfers to other sub-processors outside the EU are governed by SCCs approved by the European Commission.

17. * Measures to ensure security of processing

At the CPVO, personal data is stored in secure IT system according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. The information is stored securely so as to safeguard the confidentiality and privacy of the data.

All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement. DocuSign provides full document encryption to ensure the privacy of data. Documents stored in our ISO 27001 and SSAE 16 data centers are encrypted with the highest levels of encryption.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Certification Procedure

2. * Last update of this record:

12/03/2021

3. Reference Number:

No 33

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The processing operation concerns the certification Procedure comprises of the following stages:

Each year, in consultation with the Joint Certification Committee, the Appointing Authority of the Office determines the number of officials to be authorized to take part in the training program referred to in Article 45(a)(1) of the Staff Regulations of Officials. Following that decision, the Appointing Authority publishes a call for application. After having applied, candidates shall be pre-selected provided they meet certain conditions. A draft list of officials who have been admitted to the certification procedure is published by the Appointing Authority, who ranks the admitted candidates on the basis of a preselected criteria. The Appointing Authority shall then establish two lists: one list combines merit and level of education; a second list combines merit and recent professional experience. The highest-ranked applicants on the two lists, down to a ranking decided according to the number of posts determined, are pre-selected. A draft list of admitted applicants and a draft list of the pre-selected applicants are then published. Officials who have applied and believe that they meet the criteria but who are not included on the list, and officials who contest the number of points obtained on the basis of the criteria referred above, may appeal to the Joint Certification Committee within ten working days of the publication of the list. The final lists of admitted and pre-selected applicants is then published by the Appointing Authority.

The Appointing Authority identifies pre-selected applicants who are allowed to follow the training program. Each Head of Unit and service provides an opinion on each of the pre-selected officials and communicates it to the Head of Human Resources who shall publish the list of the applicants having reached or passed the threshold. All pre-selected applicants shall be notified of the number of points and of their ranking. Pre-selected candidates who contest the number of points obtained may appeal to the Joint Certification Committee within ten working days of the publication of the list. On the basis of the proposal of the Committee, the Appointing Authority adopts the final list of officials authorized to take part in the training program. This list is published by the Head of Human Resources.

The CPVO has concluded a Service Level Agreement with the European School of Administration (EUSA) and the European Personnel Selection Office (EPSO) authorizing the EUSA to draw up and organize the certification training program and the content of the written and oral tests respectively. The CPVO discloses to EUSA the personal number, name and surname, office telephone number, e-mail address, as well as the language of recruitment of the candidates authorized to attend the training program. EUSA will inform the CPVO of the result of the training program (absences of candidates and if they passed or failed). Only candidates whom EUSA certifies as having followed the program shall be authorized to sit the tests. Once the candidates have completed the trainings and tests, the EPSO establishes a list of officials having passed the tests; the list is then published in the CPVO by the Appointing Authority.

8. * Purpose(s) of the processing and legal basis:

The purpose of processing is to enable the selection of officials from the AST function group, from grade 5 and up, to be authorised to participate in trainings in the certification procedure framework, which will give them the possibility of being appointed to a post in the same grade in the AD function group.

Legal Instruments:

- Article 45(a) of the Staff Regulations of Officials;
- CPVO Decision of 1 June 2010 laying down the general provisions for implementing the certification procedure (Article 45(a) of the Staff Regulations of Officials);
- Service Level Agreement between the CPVO and the European School of Administration (EUSA).

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Officials of the CPVO, employed in grade 5 upwards of function group AST who have been appointed to a permanent post in the CPVO in accordance with Article 1(a) of the Staff Regulations and who, on the date of publication of the call for applications, are seconded in the interests of the service or whose administrative status as referred to in Article 35 of the Staff Regulations is one of the following: active employment, parental leave or family leave.

10. When and how were the data subjects informed:

The Privacy Statement is available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected:

- Name and surname;
- Personal reference number;
- Language competencies (mother tongue, language chosen for the training and professional situations where language was used);
- Priority area;
- Level of education and training including diplomas of higher education and trainings attended;
- Preferred training location;
- Professional experience (including within the CPVO and outside the CPVO);
- Signature of the staff member concerned.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725. In order to access personal file in paper form or rectify, block, object and erase his/her personal data kept in personal file, data subject must submit a written request to the CPVO data controller, Head of Administration Unit, at dpo@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Electronic copies of documents containing personal data are strored in the internal database Docman. Hard copies of personal files of each staff member concerned are stored in locked cupboards at the premises of the Human Resources sector and accessible only to authorised staff members of the Human Resources sector on a *need-to-know basis.*

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal and external recipients of data will have access to the data on a *need-to-know basis.*

Internal recipients:

- The Appointing Authority;
- The Heads of Unit;
- The Human Resources sector;
- IT System Administrator;
- Joint Certification Committee.

External recipients:

- European School of Administration (EUSA);
- European Personnel Selection Office (EPSO).

The external recipients may have access to name, surname, office telephone number and e-mail address.

In case of complaints, data may be disclosed to authorised persons involved in the litigation procedure.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data, including evaluation reports, promotions and reclassification decisions, will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organizations.

17. * Measures to ensure security of processing:

The physical personal files locked in the cupboards can only be accessed by the Human Resources sector. Access to electronic personal files within Docman is password-protected and can be accessed by concerned staff, Human Resources sector and IT System Administrators on a *need-to-know* basis. All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Reimbursement of Costs for Children Day-Care Centres

2. * Last update of this record:

25/03/2021

3. Reference Number:

No 34

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

When requesting for a reimbursement of one of the services, the staff member has to fill in an application form. CPVO Staff members concerned are asked to prepare their requests for reimbursement every three months. With each request for reimbursement, the staff member produces a proof of payment (a salary slip or an invoice with all the details included) and the information about the amounts already received from the "Caisse d'Allocations Familiales" or any other private body. Data are also collected from the invoices or payslips to the period for which the reimbursement is requested.

When requesting the reimbursement for the first time for maternal assistant, the staff member provides a copy of the contract and a proof that the maternal assistant is registered with the "Direction Sociales et de Solidarité (DISS) du department". This information is collected only once and is valid for subsequent reimbursements.

The documents collected by the Human Resources sector are transferred to the Accounting and Finance sector. The Accounting staff member prepares a calculation sheet in excel, where the total amount spent with the crèche/garderie facilities/maternal assistant/nursery school/day care centre are calculated.

The internal tool used by the Office to create the document concerning reimbursement of expenses is the SIFI software.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing operation is to reimburse the costs incurred by an Official, Temporary or Contract Agent employed by the CPVO for the services of "crèches" and "garderie" facilities, maternal assistants, nursery schools and day care centres.

Legal instruments:

- CPVO Decision on reimbursement by the Office of a proportion of the costs of crèches facilities "garderie" facilities, "assistantes maternelles", nursery schools and day care centers" of 30 October 2011.

Legal Bases:

- Article 5(1) (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);
- Article 5(1) (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

CPVO staff members using services of "crèches" and "garderie", maternal assistants, nursery schools and day care centres and children of CPVO staff members.

10. When and how were data subjects informed:

The Privacy Statement is made available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected from the application form and from the calculation sheet:

- Name and Surname; personnel reference number; function group/grade and status; signature of the staff member;
- Name and Surname, date of birth; of the staff's children;
- Type and trimester of reimbursement; period of time covered by the request;
- Preschool allowance or allowances received from the external entity;
- Total amount paid and reimbursed.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit to the email address dpc@cpvo.europa.eu by *explicitly* specifying *the request.*

13. Storage media of data:

Electronic copies of documents containing personal data are stored in the internal database Docman. Physical copies of financial documents containing personal data are stored in locked cupboards at the premises of the Accounting and Finance sector.

14. The recipients or categories of recipients to whom the data might be disclosed: Data are accessed on a need-to-know basis to the following recipients: - The Accounting and Finance sector; - Human Resources sector; - IT System Administrators (for maintenance purposes).
15. * Period of retention for the data: In accordance with Article 42(5) of the CPVO Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no proposed transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: Data stored on paper at the Accounting premises are secured within locked cupboards. Physical copies held by the Human Resources sector are stored in locked cupboards within the Human Resources premises. Regarding the security of electronic copies of files, access to Docman is username and password protected and only authorised recipients on a need-to-know basis (Accounting and Human Resources) have access to documents relevant to the described procedure. The database Docman is only accessible via the internal network (on-premises) or via the remote VPN SSL. Human Resources staff members have also signed a confidentiality agreement.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Communication Activities (including Newsletter)

2. * Last update of this record:

05/04/2021

3. Reference number:

No 35

4. * Name and contact details of the Controller:

President of the CPVO
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processors:

Presidency (Communication sector)
IT Unit

External processor:

SendInBlue

7. Description of the processing operation:

The Communication activities of the Office include a range of different publications, including sections on News, Articles, Conferences and Events, Webinars, and Newsletter on the CPVO website (https://cpvo.europa.eu/en/news-and-events). The Communication sector of the Office is under the remit of the CPVO Presidency and acts within the framework of the CPVO Strategic Plan 2017-2021. In this regard, the CPVO has implemented a CPVO External Communication and Outreach Strategy, dated 30 November 2020. The Communication sector is competent for publishing, for the sake of the public interest, relevant information on the news and activities of the CPVO, with a view to keep informed stakeholders and the public at large.

The Communication sector of the Office also publishes relevant information in the social media channels of the Office. For more information in this regard, please refer to Record No 12 Social Media.

Regarding particularly the CPVO newsletter, it can be sent to subscribers by email on a monthly basis, or whenever necessary from the newsletter editor point of view. It is also made available and can be consulted or/and downloaded on the CPVO website.

In order to receive the newsletter by email, a person must subscribe via CPVO website or by clicking in a subscription link made available on social media or other electronic communication. A person willing to register will have to provide her/his email address in the dedicated subscription field. The registration will be effective after the person receives and accepts a confirmation email sent by SendInBlue.

The mandatory personal data (e-mail address) is needed to ensure the delivery of the service to the subscriber, as the newsletter is sent by email.

Further to the newsletter, the CPVO at times, will need to send via email other important information to its stakeholders and registered users of the CPVO system, in the framework of the strategy of communication of the activities of the CPVO to stakeholders and EU citizens.

8. * Purpose(s) of the processing and legal basis:

The processing activity is necessary to keep stakeholders and the public at large and informed about the news and activities of the CPVO, including via the newsletter. Regarding the CPVO newsletter, an updated register with all the current subscribers of the newsletter must be kept.

Legal Instruments:

- CPVO External Communication and Outreach Strategy of 30 November 2020;
- CPVO Strategic Plan 2017-2021.

Legal Basis:

For the sending of important information to stakeholders or registered users at the CPVO:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

For the sending of the CPVO Newsletter:

- Article 5.1 (d) of the Regulation (EU) 2018/1725 (the data subject has given consent to the processing of his or her personal data for one or more specific purposes).

9. Description of the category(ies) of data subjects:

Relevant stakeholders and subscribers to the CPVO Newsletter. Also, on certain occasions, parties to proceedings.

10. When and how were data subjects informed:

The Privacy Statement is publicly available on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data:

Data collected is the e-mail address of subscribers to the newsletter.

As regards data collected from stakeholders and registered user of the CPVO System, please refer to Record No 74 Online Application System.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject rights are foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725. The data subject has the right to unsubscribe from receiving a newsletter anytime by following the link next to the newsletter subscription field on the CPVO website. In other cases, a written request should be submitted to the CPVO data controller, the President of the CPVO, at dpc@cpvo.europa.eu by *explicitly* specifying the object of the request.

13. Storage media of data:

Newsletter:

The personal data (in this case, the mailing list for the newsletter) is stored in SendInBlue, and a copy is extracted on a monthly basis and kept by the CPVO. The hosting servers on which SendinBlue processes and stores its databases are all located within the EU, on SendInBlue servers, on Google Cloud or on Amazon Web Services. SendInBlue also rents storage bays in French datacenters (Online's DC2 and DC3 datacenters located in Vitry-sur-Seine, in the region of Ile-de-France), and the hardware used is owned solely by SendinBlue. Data is stored either on Google Cloud in Belgium or on Amazon Web Services in Ireland.

Other important information:

Data on relevant stakeholders and registered parties to proceedings are stored in the contact database from the CPVO. Regarding SendInBlue's storage media of data, *see above* under the newsletter section.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data is disclosed to internal and external recipients based on the *need-to-know* principle.

Internal recipients:

The Communication and IT sectors of CPVO will have access to the email address of subscribers, including the register of current subscribers (stored in Drupal server) as well as to the new lists of subscribers that will be extracted monthly from SendInBlue, to manage the sending of the newsletter to those subscribers that have consented to it. The communication sector will have access to the email address of relevant stakeholders and registered parties to proceedings at the CPVO to send important information (such as information on the new Fee Regulation or on the COVID pandemic and the postponement of time limits).

External recipients:

SendInBlue (and its sub-processors, including Google Cloud and AWS for hosting servers as well as the other sub-processors, SendinBlue INC (US), Zendesk (US), Silverline (India) and SendInBlue Canada Inc (Canada) will only have access to the email address of subscribers to the newsletter, as well as to the email address of relevant stakeholders and registered users identified by the CPVO as necessary recipients of important notifications.

15. * Period of retention for the data:

Newsletter:

E-mail addresses are kept until the data subject decides to unsubscribe. Where the data subject unsubscribes, the personal data are permanently deleted from the mailing list and from the CPVO Register of current subscribers.

Personal data processed by SendInBlue on behalf of the CPVO are kept until the data subject decides to unsubscribe. In that case, the Communication or IT Unit promptly delete the data from SendInBlue.

Other important information:

As regards data on relevant stakeholders and registered parties to proceedings, in accordance with Article 2 of the "Decision of the President of the Office on the form of Registers kept by the Office, retention and the keeping of files including documentary evidence, publication of the Official Gazette", in case a title is granted, data will be kept for a period of 30 years from the expiry of the granted Community plant variety right. Otherwise, it will be kept for a period of 10 years following the date of rejecting the application or the date of the withdrawal of the application or the date on which the Office informs the applicant that the Office considers the application abandoned.

SendInBlue will process personal data on behalf of the CPVO as long as the contract with SendInBlue is in force, taking into account the applicable retention periods mentioned in the above paragraph. At any

time, the CPVO (either the Communication or IT Unit) can delete data from SendInBlue with immediate effect.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: Even if SendInBlue stores the data within the European Union, the following subsidiaries will process the data (email address): SendinBlue INC (US), Zendesk (US), Silverline (India) and SendInBlue Canada Inc (Canada). In this respect, further to the fact that there is an adequacy decision from the European Commission concerning private companies in Canada, SendInBlue has also signed DPA and SCC as appropriate safeguards with those subsidiaries.
17. Measures to ensure security of processing: Personal data is stored in the CPVO in secure IT system according to the security standards of the CPVO. The IT System and servers are password-protected accessible only to staff members on a *need-to-know* basis. All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement. Regarding SendInBlue, the processor takes all the necessary precautionary measures to preserve the security of the personal data. The measures are, inter alia, the following: multi-level firewall, proven solutions for anti-virus protection and detection of intrusion attempts, encrypted data transmission using SSL/https/VPN technology, Tier 3 and PCI DSS certified data centres. All data is copied at least three times in at least two different geographical locations. In the event of a catastrophic scenario, SendinBlue also regularly backs-up the data. This is encrypted before being stored in the cloud (AWS or Google Cloud). Data is backed up at least once a week and, in some occasions, even more often. Furthermore, access to processing of personal data on the behalf of Sendinblue by the receiving third-party services requires authentication of the person accessing the data, by means of an individual access code and password, regularly renewed and sufficiently robust.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Public Access Requests to documents of the CPVO Board of Appeal Register

2. * Last update of this record:

11/04/2021

3. Reference Number:

No 36

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Board of Appeal Register

7. Description of the processing operation:

Citizens of the EU and natural or legal persons residing or having their registered office in a Member State (within the meaning of Article 15 of the Treaty on the Functioning of the European Union and Article 2(1) of Regulation (EC) No 1049/2001) and, in particular, parties to legal proceedings before the Board of Appeal of the CPVO, can request access to documents held in the Board of Appeal Register, and they can also request access to documents held by Examination Offices in relation to technical examinations.

Applications for access to a document held by the Board of Appeal Register must be sent to the Office via the Office's website, by electronic mail or by post or fax to the official postal address or fax number mentioned on the website of the Office.

The Registrar of the Board of Appeal shall answer initial and confirmatory access applications within fifteen working days from the date of registration of the application. In the case of complex and bulky applications, the deadline may be extended by fifteen working days. Reasons must be given for any extension of the deadline and it must be notified to the applicant beforehand. If an application is imprecise, as referred to in Article 6(2) of Regulation (EC) No 1049/2001, the Registrar of the Board of Appeal shall invite the applicant to provide additional information making it possible to identify the documents requested; the deadline to reply shall run only from the time when the Board of Appeal Register has got this information.

The Registrar of Board of Appeal is responsible for the treatment of initial applications for access to Board of Appeal documents held in the Board of Appeal register. The applicant shall be informed of the response to its application by or under the authorization of the Registrar of the Board of Appeal. The Registrar of the Board of Appeal shall send answers to initial applications to the Chairperson of the Board of Appeal or Alternate Chairperson for information.

The decisions on confirmatory applications for access to Board of Appeal documents held in the register of the Board of Appeal shall be taken by the Chairperson of the Board of Appeal or the Alternate Chairperson of the Board of Appeal (responsible for the treatment of the confirmatory applications for access to documents).

The decision on a confirmatory application for public access to Board of Appeal documents shall be notified to the applicant in writing, where appropriate by electronic means, and inform him/her of his/her right to bring an action before the General Court.

8. * Purpose(s) of the processing and legal basis:

The processing is necessary to enable third parties and parties to proceedings with the Board of Appeal of the CPVO to request access to documents held by the Register of said Board.

Legal Instruments:

- Article 15 of the Treaty on the Functioning of the European Union;
- Article 2(1) of Regulation (EC) No 1049/2001 (Transparency Regulation);
- Articles 12 and 51 of Commission Regulation (EC) No 874/2009 of 17 September 2009 establishing implementing rules for the application of Council Regulation (EC) No 2100/94 as regards proceedings before the Community Plant Variety Office;
- Decision of the Administrative Council of the CPVO of 25 March 2004 and its amendment of 9 October 2014, on the Implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to documents;
- Amendment No 2 of 19 September 2019 to the Decision of the Administrative Council of the CPVO of 25 March 2004 and its amendment of 9 October 2014, on the Implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to documents.

Legal Basis:

Article 5.1(a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Citizens of the EU and natural or legal persons residing or having their registered office in a Member State and, in particular, parties to legal proceedings before the Board of Appeal of the CPVO.

10. How and when were data subjects informed:

The Privacy Statement is made available to data subjects on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Regarding the categories of data collected and processed from the applicant for a request for public access to documents held in the Board of Appeal Register, these are the following:

- Name and Surname, Title;
- Organisation (not mandatory);
- Professional e-mail address;
- Contact details (Postal address and phone number).

Regarding the documents to which access is granted, some personal data therein contained may be disclosed (e.g.: data on applicants for CPVR/CPVR holders). Upon the grant of the request for public access to the document, some other personal data are blanked out/blackened by default.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of the Legal service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Data is stored in the Board of Appeal Register, in the internal database Docman, at the CPVO premises.
14. The recipients or categories of recipients to whom the data might be disclosed: Regarding the application for public access and data therein contained: - The Board of Appeal Registrar; - Chairperson of the Board of Appeal or Alternate Chairperson for information. Regarding the data provided upon the grant of the request for access: - The applicant for public access.
15. * Period of retention for the data: In Accordance with the CPVO Decision on the retention of personal data which are sent by an applicant for a request of access to documents, data is deleted from the internal Docman database/filing system after a period of 24 months.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: The personal data are not intended to be transferred to any third country or international organization.
17. * Measures to ensure security of processing: The personal data is stored in secure IT systems according to the security standards of the CPVO. The information is stored securely so as to safeguard the confidentiality and privacy of the data therein. Access to the internal database Docman is username- and password-secured. Regarding incoming and outgoing traffic of electronic communications, an inbound firewall protects the system. Some personal data in documents to which access is granted further to a public access request, is blanked out/blackened. The Office uses a software called "GIMP" for this blacking out of personal data, which cannot be removed and ensure protection of the same.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controllers declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Transference of Pension Rights

2. * Last update of this record:

21/03/2021

3. Reference Number:

No 37

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processor:

PayMaster Office (PMO) (European Commission)

7. Description of the processing operation:

The processing operation concerns the transfers of pension rights: inward transfers, onward transfers and severance grant. Regarding inward transfers, the procedure allows for the transfer pension right in the Pension Scheme of the European Union Institutions (PSEUI), of pension rights acquired in one or more national schemes before starting to work within a European Institution. As for outward transfers, these allow for the transfer of pension rights acquired during the employment period in the European Institution to the national pension insurance or fund chosen by the staff member concerned. As for severance grant, this is a grant to which staff members having worked less than one year within the CPVO are entitled.

For each procedure, the staff member is required to fill in the correspondent form, provided by the Human Resources sector to the data subject upon request. It can be also downloaded within the "IntraComm" of the European Commission. Once filled out, the form is forwarded to the Human Resources sector, which will not access the documents. The document is then forwarded to the PayMaster Office (PMO) of the European Commission for the determination of the entitlements. In case of inward transfer, a proposal is made by the PMO to the staff member, subject to the acceptance (within two months) of the data subject.

8. * Purpose(s) of the processing and legal basis:

The procedure aims to convert the capital equivalent to the pension rights in the source pension scheme into pensionable years in the destination scheme.

Legal Instruments:

- Articles 70, 75, 79, 80, 81, 81a and 82 Staff Regulations of Officials;
- Articles 11, 17 to 34 of Annex VIII Staff Regulations of Officials;
- Articles 29, 34 to 38a, 97 and 103 to 108 of Conditions of Employment of Other Servants (CEOS);
- CPVO Decision of 5 October 2012 on the adoption of implementing rules to the Staff Regulations;
- Commission Decision of 20 July 2020 amending the Commission Decision C(2011)1278 of 3 March 2011 on the general implementing provisions for Articles 11 and 12 of Annex VIII to the Staff Regulations on the transfer of pension rights.

Legal Basis:

Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Officials, Temporary Agents, and Contract Agents).

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

Data subjects are also informed that additional documents are available on the "IntraComm" of the European Commission, under the PMO-4 section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

For the severance grant:

- Name and Surname;
- NUP;
- Personnel number;
- Starting and end date of the contract;
- banking information;
- Correspondence address;
- Phone number and fax number;
- E-mail;
- Signature.

For inward transfers:

- Name and Surname;
- NUP;
- Personnel number;
- Place and date of birth;
- Nationality;
- Professional address;
- Phone number;
- Email;
- Private address;
- Details of the pension scheme in respect of which a provisional calculation has been requested for the purpose of a possible transfer:
- Name of pension scheme;
- Identification number in the pension scheme;
- Address of pension scheme;
- Summary of the employment periods concerned, including contact information of the employer, start and end date of employment periods, date and signature, copy of ID proof.

For outward transfers:

- Name and Surname;
- NUP;
- Personnel number;
- Starting and end date of the contract;

- Correspondence address;
- Phone number and fax number;
- Email;
- Signature.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Physical copies of documents containing personal data are stored in the personal files of each staff member within the premises of the Human Resources sector. Electronic copies are kept in the internal database Docman.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal and external recipients have access to the personal data on a *need-to-know* basis:

Internal recipients:

- Human Resources sector;
- IT System Administrators for maintenance purposes.

External recipients:

- PayMaster Office (PMO) (European Commission);
- National public authorities (where applicable);
- Entities providing a private pension scheme (where applicable).

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member. However, these provisions do not apply to administrative data stored in the "pension" part of the personal file containing a summary of the employment history of the staff member as well as all correspondence related to the staff member with the Pension Unit of the Commission. For these data, the conservation period is extended to 10 years after the date of retirement of the (former) staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Physical copies of documents containing the requests are locked in cupboards in the Human Resources premises. As for electronic copies stored in the internal database Docman, these can only be accessed by CPVO/users from the internal network or through the remote VPN SSL. The access is further username and password protected and only concerned recipients, on a *need-to-know* basis have access to documents relevant for the procedure.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the Privacy Statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Reimbursement for Costs of Language Courses for Family members of staff

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 38

4. * Name and contact details of the Controller:

Head of the Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

In accordance with the CPVO decision of 23 March 2010, the CPVO on Payment by the Office of the cost of language courses for members of the families of the staff of the Office, the Office shall cover the costs of courses of French language or maternal language provided by a training organisation to the member of the family of a person employed by the CPVO.

The staff member wishing the CPVO to pay for a language course for a family member has to send a request to the training manager. Applications should reach the training manager at least one month before the period foreseen for the training or before the final enrolment date.

The financial support provided by the CPVO of the formal tuition in French language ceases once that the concerned family member: i) has received a total of 200 hours of tuition (in case of dependent child participating in the French school system); ii) has received a total of 80 hours of tuition (in all other cases).

The CPVO also reimburses to the staff member the fees charged by the training organisation for the provision of formal tuition in the mother tongue, preferably as a part of the group, of the child of persons of foreign nationality employed by the CPVO. The financial support provided by the CPVO in this case shall cease once the child has received a total of 100 hours of tuition.

8. * Purpose(s) of the processing and legal basis:

The purpose of the data processing is to allow the CPVO staff member to request for the financial support for language courses provided by the CPVO for his/her family members.

Legal Instrument:

CPVO decision of 23 March 2010, the CPVO on Payment by the Office of the cost of language courses for members of the families of the staff of the Office.

Legal Basis:

- Article 5(1) (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

- CPVO staff members;
- Member(s) of the family of the CPVO staff members.

10. When and how were data subjects informed:

CPVO staff members are informed by the Human Resources sector about the possibility for their family members to attend language courses.

The Privacy statement is made available to CPVO staff members in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Data subjects are requested to provide the following data:

- Nature of the training: language, duration of training, type of request;
- Reasons for attending the training.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Electronic copies of personal files and/or documents containing financial data are kept in the internal database Docman.

Physical copies are stored in the personal files of each staff member under locked cupboards at the premises of the Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

The recipients to whom the data may be disclosed include the Head of the Administration Unit, the training manager, the Human Resources sector, and the training organisation (provider of the courses).

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data in the personal file will be destroyed after a period of 10 years after the end of the contract.

As regards financial data and in accordance with Article 42(5) of the CPVO Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents are kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no proposed transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: Physical copies containing data and stored in locked cupboards at the Accounting and Finance and the Human Resources sectors' premises are accessible only to authorised staff members on a *need-to-know* basis. Regarding the security of electronic copies of files, access to Docman is username- and password-protected and only authorised recipients on a *need-to-know* basis (namely: Accounting and Finance, and Human Resources) have access to documents relevant to the described procedure. The database Docman is only accessible via the internal network (on-premises) or via the remote VPN SSL. CPVO staff members have also signed a confidentiality agreement.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Video-Surveillance System

2. * Last update of this record:

16/03/2021

3. Reference Number:

No 39

4. * Name of the Controller:

President of the CPVO
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Sector responsible for processing personal data:

IT Unit

7. Description of the processing operation:

The video-surveillance system consists in a conventional static system, which records digital images and any movement detected by the cameras in the area under surveillance, together with time, date and location. Digital images obtained from interphones (videophones at doors) are not recorded. The security guards monitor live-streaming images to control access to the buildings. All cameras operate 24 hours a day, seven days a week. The video-surveillance system complements other physical security systems (e.g.: access cards, code access and night alarms). It is part of the measures put in place pursuant to broader security policies and helps prevent, deter, if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure and/or operational information. The system is not used for any other purposes.

Access to the footage (or a copy thereof) may be granted by the President, acting as controller for the present processing, to third parties (e.g.: OLAF or local police) or to data subjects. The IT Systems Administrator (within the IT Unit) keeps a register on retention and disclosure of footages so that any disclosure or transfer of the footage. If a third party is captured on the footage, the controller informs the third party about the reasons of disclosure and asks his/her acceptance of such disclosure prior to the disclosure. The controller consults the DPO prior to any decision.

8. * Purpose(s) of the processing and legal basis:

The purpose of the use of the video-surveillance is ensuring the safety and security of CPVO 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.

Legal Instruments:

- Article 30 of Council Regulation (EC) No 2100/94 on Community plant variety rights;
- CPVO Procedure of 16 September 2019 on Video-Surveillance Policy.

Legal Basis:

Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO staff members and visitors.

10. When and how were data subjects informed:

In accordance with the EDPS Guidelines on Video-surveillance Guidelines, the CPVO Video-Surveillance Policy describes the video-surveillance system as well as the safeguards put in place to protect personal data and other fundamental rights and legitimate interests of those captured by the cameras. The Video-Surveillance Policy is adopted by the President of the Office and is available to all the staff members on the CPVO Intranet, Sharepoint.

The online data protection notice is available to the public on the CPVO website. Moreover, in each place where cameras have been installed on-the-spot notices are placed. In addition to the information that the place is subject to surveillance, the notice contains contact details of the controller, the DPO, the period of retention for the data as well as a reference to the website for the detailed notice.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

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.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, block, object and erase his/her personal data in the cases foreseen by Articles 17, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, President of the CPVO, at dpc@cpvo.europa.eu, and by *explicitly* specifying the object of the request.

13. Storage media of data:

The data is kept digitally on the hard drive of the recording machine, located within CPVO's premises.

14. The recipients or categories of recipients to whom the data might be disclosed:

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.

15. * Period of retention for the 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.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: Personal data are not intended to be transferred to a third country or international organization.
17. * Measures to ensure security of processing: 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.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), *see* the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Mobile Telecommunications Policy

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 40

4. * Name and contact details of the Controller:

Head of IT Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

IT Unit

7. Description of the processing operation:

The CPVO offers the following possibilities of mobile telecommunication devices to staff members: Basic Mobile Phone, Smart Phone, Tablet, Laptop. Staff members using mobile telecommunications services/devices are requested to give previous acceptance to the conditions laid down in the ICT user Policy.

The IT Unit is responsible for monitoring and implementing the CPVO policy and guidelines concerning the use, in the interest of the service, of mobile telecommunication services by internal/external staff members.

The telecommunication services provided are: Voice (Internal 4-digit numbers, National, Europe or International) and Data (Wi-Fi only, National, Europe or International).

Mobiles are pre-loaded with the applications necessary for normal professional use, namely RSA SecurID and Dialog. Staff members shall not carry out Office business on any other application than those provided. The user is responsible for covering any costs related to subscription/purchase for any applications that they download from an online store.

The processing of personal data is not intended to be used for any automated decision making, including profiling.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing concerns the acquisition, management and use of mobile telecommunications resources within the Office. Mobile telecommunications resources are acquired and used in response to a strategic need of the Office.

Legal Instruments:

CPVO Procedure of 1 February 2021 on Allocation and use of IT Equipment.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. Description of the category(ies) of data subject(s):

CPVO staff members gaining access to mobile telecommunication devices.

10. When and how were data subjects informed:

The Privacy Statement is made available to the data subjects in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. Description of the category(ies) of data subject(s):

CPVO staff members gaining access to mobile telecommunication devices.

12. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data processed are the following:

- Name and Surname, personal number, phone number, address (building, floor, office), start/end date at CPVO, Department for internal/external staff;
- Calling number, called number, country, date and time of call, duration of the call and cost, type of phone, SIM card number and PUK code.

13. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 submitting a written request by email to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu, by explicitly specifying the object of the request.

14. Storage media of data:

List of users, numbers and devices are stored on internals servers (on-premises Server). A dedicated file (Excel sheet) is stored on Sharepoint, containing data on reporting SIM cards, PUK codes types of phone and list of devices owned by the users.

Invoices are stored in the internal database Docman.

15. The recipients or categories of recipients to whom the data might be disclosed:

Access to the data is determined on a *need-to-know* basis. Access is provided to the following persons/services:

The concerned staff member and his/her line manager (or Head of Unit) have access to the data relating to the specific procedure of the staff member allowed to use the devices (namely: name and surname, personal number, phone number, Unit/sector, building/place of work, start and end date of contract with CPVO).

The IT Unit has access to all the data related to this processing activity to approve the requests as well as monitor and implement the CPVO telecommunication policy. IT system Administrators have also access to the list of devices owned by the user, SIM card number and PUK code. Staff members in the Accounting and Finance sector have access to the detailed invoices relating to the concerned use of devices by CPVO staff members.
16. * Period of retention for the data: In accordance with the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member. Where a user receives a new device, data contained in the old device are erased once the IT Unit receives it.
17. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: The personal data is not intended to be transferred to any third country or international organizations.
18. * Measures to ensure security of processing: All data are stored on an on-premises server, duly secured by firewalls and only accessible by the IT System Administrators. Access is also password-protected, based on Windows credentials. Only the IT Administrator is authorised and able to has access to a dedicated file (Excel sheet) on Sharepoint, reporting SIM card, PUK code and type of phone and the list of devices owned by the users. Regarding invoices stored in the internal database Docman, these are accessible only to authorised members in the Accounting and Finance sector.
19. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Assessment and Reporting on Probationary Periods

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 41

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

In accordance with Article 34 of the Staff Regulations of Officials and Articles 14 and 84 of the Conditions of Employment of Other Servants (CEOS), every newly recruited Official, Temporary Agent or Contract Agent shall serve a probationary period when taking up service. A report shall be drawn up in order to evaluate the agent during this period. A report on the probationary period is elaborated at the end of this initial period, which basically consists in an objective summary assessment of the staff member's performance, competences and conduct. This report serves as a basis for the confirmation or dismissal of the respective Official or Agent, as well as for the possible extension of the probation period.

8. * Purpose(s) of the processing and legal basis:

The procedure is necessary to enable the evaluation of Officials and of Temporary and Contract Agents during the initial period of their employment at the CPVO.

Legal Instruments:

- Article 34 of the Staff Regulations of Officials;
- Article 14 and 84 of the Conditions of Employment of Other Servants (CEOS);
- Commission Decision of 16 October 2017 on the general provisions for implementing Article 79(2) of the Conditions of Employment of Other Servants of the European Union, governing the conditions of employment of contract staff employed by the Commission under the terms of Articles 3a and 3b thereof (by analogy).

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Data subjects include all CPVO staff members (Permanent Officials, Temporary Agents, and Contract Agents) employed by CPVO on probationary period.

10. When and how were data subjects informed:

The Privacy Statement is available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The probationary report contains the following data:

- Name and Surname;
- Personal number;
- Job Title;
- Type of contract;
- Category and grade;
- Unit/Sector;
- Contract start date and duration;
- Deadline for completion of assessment;
- Hierarchical Supervisor's name and surname;
- Reporting Officer's name and surname;
- President's name and surname;
- Tasks to be performed under the contract;
- Any break in probationary period if applicable (period of absence and reasons);
- Self-assessment;
- Comments by hierarchy;
- Decision by the President.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The data are kept in the personal files for each staff member concerned in the internal database Docman. Physical copies of the personal files may be kept under locked cupboards at the Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

The data is disclosed to the President, the reporting Officer, the staff member concerned and the staff members in the Human Resources sector.

In the event the staff member concerned is dismissed, the President's decision will be transferred to the PMO.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17.	**Measures to ensure security of processing:** The files containing the probationary reports are kept in the personal file of the data subjectThe physical file is stored in a locked cupboard at the premises of the Human Resources sector, accessible only to authorised staff members of the Human Resources sector on a *need-to-know* basis. Regarding the internal database Docman, where digital copies of personal files are stored, is username and password-secured. The database Docman is only accessible via the internal network (on-premises) or via the remote VPN SSL.
18.	* **For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.**

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Email Management

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 42

4. * Name and contact details of the Controller:

Head of IT Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

IT Unit

7. Description of the processing operation:

The processing concerns the flow of electronic communications and exchange of electronic messages and attachments between the CPVO staff members and external users, such as contractors, clients, and any other stakeholders or recipients of emails sent by the CPVO. CPVO staff members are provided access to the directory of e-mail addresses of CPVO e-mail service users, including of main external partners (other Institutions and Bodies, Member States, and other EU organisations included in the email address book). A back-up of emails is also in place for those cases where the CPVO email system user requests the recovery of a deleted e-mail. The described processing is not intended to be used for any automated decision making, including profiling.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is the management of the flow of e-mail communications at the CPVO and the establishment of the retention period for e-mails and backups of e-mails (received or sent by the users of the CPVO e-mail service).

Legal instruments:

- CPVO Policy of 1 January 2020 on the Use and Monitoring of CPVO Communications and IT tools;
- CPVO Procedure of 1 February 2021 on Allocation and use of IT Equipment.

Legal basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Users of the email system of the CPVO (senders and recipients of emails to and from the CPVO).

10. When and how were data subjects informed:

The Privacy Statement is made available to the data subjects in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The personal data that are being processed are all personal data that are included in the received and send emails to and from the CPVO. More specifically:

- Name and Surname of the CPVO e-mail system users;
- E-mail addresses of both the sender and the recipient, and any address book references;
- E-mail subject, contents and attachments.

Personal data can also be included in the Address book:
- Name and Surname;
- E-mail address;
- Unit/service;
- Office location;
- Office phone number;
- Office mobile number;
- Company;
- E-mail group memberships.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The servers are kept in the premises of the Office in locked rooms.

14. The recipients or categories of recipients to whom the data might be disclosed:

Regarding the Address Directory, all CPVO staff members have access to it.

Regarding e-mail exchanges, data may be disclosed to CPVO staff members and external users. Data may also be disclosed to IT Administrators on a *need-to-know* basis.

15. * Period of retention for the data:

Personal data is kept only for the time necessary to keep the emails of the CPVO staff members in their mailbox or personal e-mail archive. Information in the address book will be maintained for as long as a user has a contractual commitment to the CPVO and/or communication is deemed to be necessary due to the nature of the established relationship.

In the event of termination of the contractual or any other commitment of the user with the CPVO, the user inbox, address book entries and information, stored in e-mails, will be maintained for one month from the date of end of the contract.

Data stored as Back-up will also be maintained for one year from the date of the digital exchange, with a view to give users the opportunity to recover any e-mails that have been deleted or lost.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organization.

17. * Measures to ensure security of processing:

The CPVO puts in place appropriate technical and organisational measures to safeguard and protect the processed personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to it. All personal data relating to the management of emails is stored in secure IT applications (exchange servers). The servers are password-protected, and the inbound and outbound communication traffic is protected by firewalls.

The Office premises, including the location where the servers are stored, are safeguarded by the Security team of the Office, implementing a number of security measures.

Appropriate levels of e-mail access are granted individually only to authorized recipients, that is, to staff members responsible for the concerned processing operation, based on legitimate and specific business purposes. E-mail access is username- and password-protected under single sign-on system and automatically connected to the user ID.

IT Administrators also act, within the remit of their functions at the Office, under the duty of confidentiality and have signed a declaration of confidentiality.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Contacts Database

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 43

4. * Name and contact details of the Controller:

President of the CPVO
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

- President of the CPVO;
- Administration Unit;
- Technical Unit;
- IT Unit;
- Legal, Procurement and Logistic service.

7. Description of the processing operation:

The processing operation consists in gathering and storing in the CPVO internal Contacts database the name and contact details of clients, CPVO staff members, CPVO external contractors, suppliers, affiliated parties (such as experts and employees of Examination Offices), National or International Organizations, members and Observers of the CPVO Administrative Council, of members of the CPVO Decision Committees, as well as of any other user of extranet services.

Data gathered into the Contacts database includes data originating from the initial registration by users in the User Area. The User Area is a professional and secure restricted electronic platform that consists in a series of web pages requiring user's authentication, only accessible via a personalized account, providing identified users with access to user-related information and online tools. In essence, the User Area is a unique entry point in the Official CPVO website (www.cpvo.europa.eu).

CPVO staff members may as well manually introduce or amend data in the Contacts database for the performance of the required tasks within the remit of the Office.

8. * Purpose(s) of the processing and legal basis:

The processing operation is necessary for the well-functioning of the Office in the performance of tasks in the public interest.

Legal Instruments:

- Articles 87 and 79 of the Regulation (EC) No 2100/94 on Community plant variety rights;
- Article 64a (2) of the Commission Regulation (EC) No 874/2009;

- Terms & Conditions concerning electronic systems of communication with and by the Office as established in decision of the President of the CPVO.

Legal basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Users, CPVO staff members, CPVO external contractors, suppliers, affiliated parties (such as experts and employees of Examination Offices), National or international organisations, members and Observers of the Administrative Council and of members of the CPVO Decision Committees and any other user of extranet services.

10. When and how were data subjects informed:

Depending on the specific processing operation based on which data has been stored in the Contacts database, the concerned respective Privacy Statement is made available to the data subjects at the time of collection of the personal data.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data that are collected directly from the data subject is:

- Name and Surname;
- Company;
- Title;
- Phone number;
- Email address;
- Postal address / Country.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the data Controller, the President of the CPVO, at dpc@cpvo.europa.eu, by *explicitly specifying* the request.

13. Storage media of data:

The data are stored in the Contact database, in servers at the CPVO premises in Angers (France).

14. The recipients or categories of recipients to whom the data might be disclosed:

Only authorised CPVO staff members have access to data stored in the Contacts database.

15. * Period of retention for the data:

Depending on the specific processing activity underlying the need to store the data in the Contacts database in accordance with the concerned applicable statutory decision of the President of the CPVO, data may be kept as long as necessary for the purpose of such processing activity.

16. * Proposed transfers of data to third countries or international organizations, and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organisation.

17. * Measures to ensure security of processing: Personal data are stored in the Contacts database in conformity with the security standards of the CPVO. Access to the database is username- and password-protected, and requires the professional device to be connected with the VPN remote server of the CPVO. The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate *need-to-know* basis for the purpose of this processing operation. All CPVO staff members must sign a confidentiality declaration and non-disclosure agreement at the time of signing their employment contract with the Office.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Management of Requests for Part-Time Work

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 44

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processor:

SYSPER 2 (European Commission)
PayMaster Office (PMO) (European Commission)
DG DIGIT European Commission

7. Description of the processing operation:

The processing operation concerns the grant of authorisation to work part-time under the conditions laid down in Article 55(a) and in Annex IVa of the Staff Regulations. The applicant fills in a part-time request in the TIM module in SYSPER. The request will determine the type of the part-time work, its beginning, its duration and the daily work schedule. Data subjects may be asked to present supporting documents to the request in the case the part-time is requested for family or medical reason. Data is used by the PMO for salary calculation purpose. The result of this calculation will appear on the salary slip.

Data are also processed in the CAR module in SYSPER, covering basic procedures for the management of career and mobility of staff members. The module is based on an events-engine ensuring consistency of the career history of staff members. For more information, please refer to Record No 68 SYSPER.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is the management of part-time applications of the CPVO staff members, allowing them to work part-time under the conditions laid down in Article 55 (a) and in Annex IV a of the Staff Regulations.

Legal instruments:

- Annex IVa of the Staff Regulations of Officials;
- The Commission Decision on part-time work of 8 January 2016;

- Article 16, 19, 91 and 92 of the Conditions of Employment of Other Servants of the European Union (CEOS).

Legal Basis:

Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

The CPVO staff members, including Officials, Temporary Agents, and Contract Agents.

10. When and how were data subjects informed:

The Privacy Statement for the management of requests for part-time work is available on the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

The Privacy Statements of the TIM and CAR modules in SYPER, are both also available to all staff members in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The part-time request contains the following data:

- SYSPER Identification data, including name, surname, NUP and job number;
- Exact period of part-time work requested and whether it is a new request or a renewal (it includes exact days or half-days off in case of special part-time);
- Type of part-time work (in case of parental leave, also name and surname, age of the child and if handicapped; in case of family leave, also name and relationship with family members and postal address);
- Time credits;
- the chosen percetange for the part-time work;
- Pension contribution;
- further supporting document justifying the request, as medical certificate, request for training.

In the event the supporting documents justyfing the request contain relate to medical data, SYSPER does not process direct medical data of CPVO Staff members or her/his family members, just administrative data related to the request.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

All data are stored in SYSPER, in the individual profile of the staff member (including the supporting documents).

14. The recipients or categories of recipients to whom the data might be disclosed:

Data is disclosed to internal staff members and the service provider on a *need-to-know* basis.

Internal recipients:

- Staff's Line Manager;
- The Appointing Authority;
- The Human Resources Sector.

External recipients: - SYSPER 2 (European Commission) for the purpose of carrying out the service; - PayMaster Office (PMO) (European Commission) for the purpose of salary calculation; - DG DIGIT European Commission for maintenance purposes.
15. * Period for retention for the data: Please refer to Record No 68 SYSPER and the privacy statements of TIM and CAR modules.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no proposed transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: Please refer to Record No 68 SYSPER.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Events and Meetings

2. * Last update of this record:

07/04/2021

3. Reference Number:

No 45

4. * Name and contact details of the Controller:

President of the CPVO
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processora:

CPVO Presidency
Technical Unit

External processors:

Event Drive and its sub-processors
Microsoft and its sub-processors

7. Description of the processing operation:

Both the CPVO Presidency and the Technical Unit organize events such as the Administrative Council meetings or the Examination Office meetings. In order to organize such events, the staff responsible for organizing the event first identifies the list of potential participants and then extracts said list from the CPVO Contacts Database. The invitations are then sent by email by the staff organizing the event, through the dissemination of registration forms that are sent either by email/post/external platform Eventdrive and which must be filled and returned by the participants.

In case the platform Eventdrive is used to send the invitations, the name, surname and email address of the potential participants is then exported to the platform, who then sends the invitation to the email addresses, including a link for registration.

Scientific opinions and views may be provided in meetings and discussion panels and minutes may be kept during meetings and, in some occasions, also audios may be recorded. Translation services may Photos may be taken during the event by the Communication sector and published for internal or external communication purposes.

Data subjects are duly informed on the possibility that photos might be taken by the CPVO. In this respect, as for the meetings of the Administrative Council, data subjects receive the relevant information in the e-mail of invitation to the meetings and events organised. They are informed that photos might be taken

and could be published on social media for communication purposes. They are also informed before the photo session takes place and they can opt not to be part of it.

Due to the outbreak of the coronavirus COVID-19 pandemic, the Office has extended the use of 'Microsoft Teams' ('MS Teams'), as part of Microsoft Office 365, to organise virtual meetings and videoconferences remotely with internal staff and external stakeholders, including events and meetings organized by the CPVO. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the above-mentioned services.

8. * Purpose(s) of the processing and legal basis:

Personal data are processed for organising and managing events, for coordinating any required follow-up activities, and for accountability and communication/transparency purposes. This may include registration for event participants, logistic support before and during the event, minute-taking and distribution of minutes, web-publication, and enabling the CPVO to provide participants with further information on particular meetings/events in the future.

Depending on the nature and scope of the event, audio recordings may be taken for the purpose of drafting the minutes.

Photos may be taken for internal and external communication purposes. Internal purposes are the following: a) informing the CPVO Staff Members on activities carried out by the Office via the blog "Staff News", available on Sharepoint and only accessible by CPVO Staff Members; b) historical archiving, namely, storage of photos related to specific historical events involving the CPVO (such as the 20th anniversary of the CPVO). External purposes refer to the promotion of the CPVO to the public through social media.

The processing of personal data is not intended to be used for any automated decision making, including profiling.

Legal instruments:

- CPVO External Communication and Outreach strategy of 30 November 2020;
- CPVO Internal Communication Policy of 30 November 2020;
- CPVO Social Media Policy of 1 January 2020.

Legal bases:

- Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

Regarding particularly the taking of pictures:
- Article 5.1 (d) of Regulation (EU) 2018/1725 (the data subject has given consent to the processing of his or her personal data for one or more specific purposes).

In any case, it must be noted that for the processing operations of photos taken in exceptional circumstances, such as events of historical relevance (e.g.: the 20th anniversary of the CPVO), the legal basis is Article 5.1 (a) of the Regulation (EU) No 2018/1725.

9. * Description of the category(ies) of data subject(s):

Participants in the events and/or meetings, organised by the CPVO. Participants to the event are CPVO external stakeholders and staff members of the entrusted Examination Offices.

10. When and how were data subjects informed:

The Privacy Statement is published on the CPVO website and is also made available to data subjects along with the invitation to the event. Data subjects are duly informed about the possibility of taking pictures in the e-mail of invitation to the events. Likewise, where audio recordings are being made, data subjects are informed in the invitation letter and confirmation of attendance.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following personal data of the participants to events are processed:

- Name and Surname
- Postal Address
- Telephone
- E-mail
- Country
- Official Position
- Organisation/Company
- For speakers: CV and photo

When processing the data during the organisation of meetings via MS Teams, the following personal data are also processed:

- Electronic identifying information: IP address, cookies, connection data and access times;
- Movie, pictures, video and audio recordings;
- Metadata used for the maintenance of the service provided;
- Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contact and similar).

There might be photos of the participants taken during the event. Consent will be requested to participants before the taking of any photographs at the beginning of the event. They will also be informed of the foreseen use of said photographs. Any participant not wishing to be photographed can express it and accordingly not appear on the picture.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EC) No 2018/1725 by submitting a written request to the CPVO data controller, President of the CPVO, at dpo@cpvo.europa.eu, by *explicitly* specifying the object of the request.

The data subject can also submit a request to the service provider Eventdrive to exercise his/her right. In this case, please refer to the privacy policy of Eventdrive, available at: https://www.eventdrive.com/en/legal/privacy-policy.

13. Storage media of data:

CPVO:

Photos taken for internal communication purposes are stored in the Intranet of the Office, Sharepoint. The CV and photo of speakers are stored in the professional device of the staff members responsible for the organization of the event.

Personal data of the participants are stored in the Contact Database of the CPVO. For more information, please refer to Record No 43 Contacts Database. Photos taken for external communication purposes may be stored on the CPVO webpage and social media. For more information, please refer to Record No 12 Social Media.

External processors:

As regards the external processor Eventdrive, personal data of participants (in this case name and surname, and e-mail address) are stored in servers held by Eventdrive and located in France.

As regards external sub-processors of Eventdrive, namely, "SendGrid" and "Twilio", personal data of participants (in this case, only e-mail address), as part of the transactional e-mails sent on behalf of the CPVO by Eventdrive, are stored by Sendgrid within Twilio's facilities, in the United States.

As for Microsoft, data is stored in Europe. However, additional data may be available to sub-processors outside the EU (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

The CPVO Staff members in the Presidency or in the Technical Unit which are in charge of organizing the events will have access to all personal data processed in the organization of the event. The IT Unit will have access on a *need-to-know* basis for maintenance purposes as well as CPVO IT Unit's external service provider from Uplink.

External recipients:

The processors Eventdrive, SendGrid and Twilio will only have access to the name and surname, and email address of the participants to the event.

As regards photos taken for external purposes, please refer to Record No 12 Social Media.

As regards the use of Microsoft Teams, Microsoft and its sub-processors will have access to personal data in order to provide maintenance, support or operation of the online service.

15. * Period of retention for the data:

CPVO:

As regards data on participants kept in the Contact database, please refer to Record No 43 Contacts Database.

As for photos taken during events and meetings for external purposes, data will be retained as long as the data subject does not withdraw the consent. However, in exceptional circumstances (i.e. events of historical relevance as the 20th anniversary of the CPVO), data may be retained for a longer period.

Eventdrive, Microsoft and their sub-processors:

As regards Eventdrive, data are retained for active accounts as long as it is necessary and relevant to run the service. Eventdrive may retain information from closed account to comply with the law, prevent fraud, resolve disputes, assist any investigation and take other actions permitted by the law.

As for Sendgrid and Twilio, personal data is automatically deleted after one year on Twilio's networks upon termination of the agreement between Eventdrive, Sendgrid and Twilio. Twilio may retain personal data or a portion of it if required by the applicable law, provided that it remains protected in accordance with the applicable data protection law and the terms of the agreement between Eventdrive, Sendgrid and Twilio.

As regards MS Teams, data will be stored in MS Teams for one year after the exchange activity is completed.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

As for events and meetings, personal data may be transferred to third countries by sub-processors of Eventdrive. Even if Eventdrive stores the data in the European Union, the following subsidiaries will process the data: Twilio and Sendgrid, both located in United States. Sendgrid and Twilio are subject to Sec. 702 FISA, a US Surveillance law. Eventdrive signed a Data Protection Addendum incorporating Standard Contractual Clauses as appropriate safeguards with those sub-processors. Data processed are name and surname, and e-mails of participants to the events.

As regards the use of Microsoft Office 365 and online applications, most customer data is kept in Europe, but additional data may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

In particular, regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by CPVO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

As for the other personal information addressed in the present processing activity, there are no proposed transfers to third countries.

17. * Measures to ensure security of processing:

At the CPVO, personal data associated with the organisation, coordination and follow-up of the event is stored in secure IT systems according to the security standards of the CPVO. CPVO systems and servers are username- and password-protected. All persons dealing with personal data in the context of the IT Systems sign at some stage a confidentiality declaration and/or non-disclosure agreement.

Eventdrive stores personal information in secured and encrypted databases, not connected to the open internet. The database cannot be accessed without establishing a secured and authenticated connection with Eventdrive' servers. Data in transit are further secured with the use of API and SMTP.

Sendgrid and Twilio take all the precautionary measures to preserve the security of personal data. The measures are, inter alia, the following: Data centres have SOC2 Type 2 reports, a dedicated team monitoring suspiciours activities and operational security measures. The latter, in particular, refers to background check for emplyees, signed confidentiality agreements, termination/access removal process, acceptable user agreements. Data in transit are further secured with the use of API and SMTP.

As regards Microsoft Office and MS Teams, Microsoft 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 them. Office 365 has been configured to preserve the confidentiality of the information you exchange by implementing encryption during all communications and in storage, and anonymous access is not authorized. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. Datacentres have physical and logical security monitoring measures. Finally, Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Activities of the CPVO Staff Committee

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 46

4. * Name and contact details of the Controller:

The Chair of the Staff Committee
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Staff Committee

External processors:

Comitéo https://www.comiteo.net/
Cezam https://www.cezam.fr/cezam

7. Description of the processing operation:

The Staff Committee of the CPVO process personal data on 5 main occasions as listed below:
1- Promotion and Reclassification of current CPVO staff member(s);
2- Recruitment of new staff member(s);
3- Correspondence between staff member(s) and Staff Committee;
4- Social gatherings;
5- Subscription to other services including Cezam, Comitéo, sport activities.

1- During each promotion and reclassification procedure, documents as personal files of Staff member concerned and comments made by the participants are produced and disclosed by Human Resources sector to selected members of the Staff Committee, as the body is required to appoint representatives for the procedure. The Human Resources Sector grants a temporary limited, restricted access on Sharepoint to these documents to selected members of the Staff Committee.

2- During recruitment procedures of staff members, a Staff Committee member or other member of the staff nominated ad hoc, as part of the Selection Committee, receives the CVs and the motivation letters of the candidates for use only during the interview of the candidates. They are then destroyed. In particular, the Human Resources sector grants a temporary limited, restricted access on Sharepoint to these documents to selected members within the Staff Committee. Once the selection procedure is completed, access to these documents is not anymore available. If electronic copies or hard copies are produced, they are destroyed/deleted once the procedure is over.

3- Any staff member may contact a Staff Committee member to express an opinion, discuss any matters or put forward any suggestions. Correspondence with the said staff member who might disclose personal data, sensitive or not, is done orally or via internal emails. Those emails are kept within the Staff Committee member's professional email, the access to which is password-secured. Furthermore, the members of the Staff Committee may draft notes, advice(s), minutes of meetings in the context of other duties such as, for instance, submitting suggestions to the management, putting forward proposals to enhance the staff working (and living) conditions, voicing concerns over the application and/or interpretation of the Staff Regulations.

4- When the Staff Committee's members prepare any social event, such as the Christmas celebration with the staff families, they ask for specific personal data related to the composition of the staff member's family (children, partner, etc.). These data are exchanged either directly between the staff members and the Staff Committee, orally, or by email with the Human Resources sector or the staff members. The emails are deleted after the organisation of the event.

5- As one of the Staff Committee's duties is to provide suggestions and proposals concerning empoyees' working and living conditions, the Staff Committee may propose the subscription to certain external services. The subscription to these services may entail the transmission of personal data of staff members to external organisations or professionals (e.g.: "Cezam", "Comitéo", professional trainers). The data transmitted would consist of the name, surname, personal or professional email of the staff member, as well as, in some occasions, of the composition of the family members.

Photos may be taken during the events organized by the Staff Committee by the Communication sector and published for internal or external communication purposes. Internal purposes are the following: a) informing the CPVO Staff Members on activities carried out by the Office via the blog "Staff News", available on Sharepoint and only accessible by CPVO Staff Members; b) historical archiving, namely, storage of photos related to specific historical events involving the CPVO (e.g.: the CPVO's 25th anniversary). External purposes refer to the promotion of the CPVO to the public through social media. As for the processing operations regarding photos taken for external purposes, please refer to Record No 12 Social Media.

8. * Purpose(s) of the processing and legal basis:

The processing of data is necessary to fulfil the duties of the Staff Committee which are established in the CPVO Decision of 15 March 2017 on the setting up a Staff Committee. In particular, the Staff Committee represents the interests of the staff vis-à-vis the CPVO and provides a channel for expression of opinions by the staff. This includes enabling staff members to voice concerns relating to the application and interpretation of the Staff Regulations, to present proposals for the improvement of staff working conditions or general living conditions, and to submit suggestions to the President concerning the organisation and operation of the CPVO's services. Finally, the Staff Committee appoints representatives during the selection, promotion or reclassification procedures.

Legal Instruments:

- CPVO Decision of 15 March 2017 on setting up a staff a Staff Committee;
- CPVO Decision of 17 July 2016 laying down general implementing provisions regarding Article 45 of the Staff Regulations;
- CPVO Decision of 17 July 2016 on Reclassification of Temporary Agents;
- CPVO Decision of 17 June 2016 on Reclassification of Contract Agents;
- CPVO Decision of 8 June 2011 on the retention policy for the working documents of the members of the Staff Committee;
- Article 9(3) of the Staff Regulations.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).
- As regards the taking of photographs during external social events and services (see above point 7, No 4 and 5), please refer to Record No 12 Social Media.

9. * Description of the category(ies) of data subject(s):

- All CPVO staff members;

- Candidates to a CPVO vacancy;
- Family members of CPVO staff members, in the case of social events.

10. When and how were data subjects informed:

The Privacy Statement is available to CPVO staff members in the CPVO Intranet, Sharepoint, under the Data Protection Officer section. As regards the taking of photographs during external social events and services, the corresponding Privacy Statement is made publicly available on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Personal data from Human Resources personal files concerning assessments for the reclassification or promotion of CPVO staff members. In particular, name and surname of the staff member concerned, grades, steps, date of last promotion/reclassification, the average career plan, contract duration, job assignment, promotion/reclassification threshold, including accumulated capital of points since the last promotion/reclassification, number of promotion/reclassification points proposed/awarded in the current exercise (including specific merit points), total number of promotion/reclassification points and number of promotion/reclassification in the past promotion/reclassification exercise.

- Family-related data, which is processed in the context of the organization of social events and other activities (see above point 7 No 4 and 5). The data collected are: name and surname, email address (professional or private) of the staff member concerned, number of children and the age of such, as well as the presence of the partner.

- CVs and motivation letters from candidates to a CPVO vacancy.

- Opinions, questions put forward by staff members or suggestions expressed to the Staff Committee (which may contain personal data).

- As regards the external processor Cezam, the data collected are: name and surname, birthdate, email address (professional or private) of the staff member concerned, number of childrens and their age, name and surname of the partner (in some cases, only the presence of the partner), the number of the Cezam Card, reference product bought, price and fees (related to the use of the Cezam Card), connection and browsing data might also be gathered, including IP address, login and password, and logs.

- As regards the external processor Comiteo, the data collected are: name, surname, email address (professional or private) and postal address of the staff member concerned, social security number, status of the user, activity of the user within the website, IP address and browser used by the CPVO staff member, seniority steps within the CPVO, banking information.

- Trainers, in the context of sport activities, may have access to the name, surname and email address of the Staff member involved.

In exceptional circumstances, within the framework of the organization of social gathering events (see above point 7 No 4), sensitive data as dietary requirements and information on possible allergies may be gathered orally by the Staff Committee member in charge of the event.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725, by submitting a written request via email to the data Controller, the Chair of the Staff Committee, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Physical copies of personal files, CVs and Motivation letters, made available by the Human Resources sector to the selected Staff Committee member(s) (or in his absence, alternates), are stored within staff member's own office and destroyed once the selection procedure/assessment procedure is concluded. Likewise, in the case of electronic copies stored on the professional device of the Staff Committee member, these are deleted once the selection procedure or the assessment is finalized.

Email exchanges regarding suggestions and opinions on decisions (see above point 7 No 3) are stored either in the "functional emailbox" of the Staff Committee, or in the personal professional emailbox of the Staff Committee member. Notes and minutes of meetings are stored on Sharepoint and are accessible only by CPVO staff members.

Contracts signed with service providers as Cezam and Comitéo are only physically stored within the procurement service and may be accessed only by procurement staff members.

As for the storage of personal data of candidates to CPVO vacancy, namely, CVs and motivation letters, as well as personal data from Human Resources personal files for the purpose of staff member's promotion or reclassification, please refer to Record No 72 e-Recruitment and Record No 7 Promotion and Reclassification of Officials, Temporary Agents and Contract Agents in the CPVO.

Data collected by the external subprocessors Comitéo and Cezam are stored within the EU.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- The Human Resources sector, in the context of promotion/reclassification procedures;
- Selected members of the Staff Committee (or alternates or staff members nominated on an ad hoc basis) on a *need-to-know* basis in the context of selection procedures, of social gathering events and subscription to external services.

External recipients:

- The external processors Cezam and Comitéo, as well as their sub-processors (Comitéo avails itself of the companies "ALTER CE" and "Saleforce" in order to provide the service);
- Trainers, in the context of sport activities.

15. * Period of retention for the data:

In accordance with the CPVO Decision of 8 June 2011 on the retention policy for the working documents of the Staff Committee, physical documents and electronic copies related to selection, promotion or reclassification procedures containing personal data and disclosed to the selected Staff Committee member(s) by the Human Resources sector, are destroyed (and erased from the Staff Committee member's device) once the selection procedure is over.

Other working documents, such as notes, advice(s), and minutes from meetings, are stored for 24 months and can be used in case of complaint(s) or appeal(s) from staff members.

Emails and written correspondence concerning suggestions addressed by CPVO staff members at the Staff Committee, either via the Staff Committee "functional emailbox" or via the private email box (see above point 7 No 3), are retained for 24 months.

Emails received in the context of the organisation of social events (see above point 7 No 4), are deleted either the day that the event takes place or promptly after the organisation of the said event.

In exceptional circumstances, for reasons of knowledge conservation and consistency across succeeding Staff Committees, documents may be retained for a longer period (e.g.: PPT for a General Assembly).

As regards personal data of candidates to a CPVO vacancy gathered in the context of recruitment procedures, as well as personal data in Human Resources personal files, please refer to Record No 72 e-Recruitment and Record No 7 Promotion and Reclassification of Officials, Temporary Agents and Contract Agents in the CPVO.

Personal data processed by Cezam will be retained as long as active users maintain their subscription to the services. However, data related to the use of the Cezam Card are retained for 5 years.

Personal data processed by Comitéo will be retained for a maximum of three years after the end of the commercial relationship.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: The personal data is not intended to be transferred to a third country or international organisation.
17. * Measures to ensure security of processing: The "functional emailbox" of the Staff Committee is username- and password-protected. Access is restricted to Staff Committee members only. The personal professional emailbox is also username- and password-protected. Dietary requirements which might be gathered in view of social events, are only collected orally by the Staff member(s) in charge of the organisation of the event. As regards the selection, promotion or reclassification procedures (point 7 No 1 and 2), the Human Resources sector provides restricted and temporary access only to selected Staff Committee members in relation to personal files (promotion and reclassification) as well as applications received by candidates to CPVO vacancies. As for the security measures adopted within the processing operations concerning the recruitment procedure and the management of personal file, please refer to Record No 13 Consultation of Personal Files and Record No 72 e-Recruitment. Cezam also adopts different security measures, *inter alia*, designation of a responsible person for the protection of personal data, adoption of secure IT System and the necessary organisational measures as training of employees, internal awareness campaigns, strict confidentialy rules for employees as well as selection of sub-processors on the basis of the ability to show compliance with the relevant laws. Comitéo adopts different security measures, in particular: certified payments via PCI and DDS, anonymization of personal data when transferred to third parties, secure connection with HTTPS with TLS 1.2 and TLS 1.3, security measures on storage with hosting sub-processors holding ISO 27001-ISO 27017-ISO27018 – SSAE16/ISAE3402 (SOC2/3), as well as security audits held regularly. Furthermore, banking information of the data subjects are encrypted.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Procurement and Grant Procedures

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 47

4. * Name and contact details of the Controller:

Head of Legal, Procurement and Logistics Service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
Email address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal, Procurement and Logistics service

7. Description of the processing operation:

The processing operation concerns procurement and grant procedures and calls for expression of interest with the Office. Data is collected and managed by the Office to evaluate the eligibility of economic operators/applicants, partners/affiliated entities and subcontractors to participate in procurement or grant procedures, and/or evaluate the content of tenders or proposals submitted during the procurement/grant procedures with a view to awarding the contract or agreement. Certain data is necessary for the execution of the contracts/agreements awarded. The processing of personal data is not intended to be used for any automated decision making, including profiling.

8. * Purpose(s) of the processing and legal basis:

The processing operation is necessary to enable the management of procurement and grant procedures and calls for expression of interest with the Office.

Legal Instruments:

- Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union;
- CPVO Financial Regulation;
- The contract or grant agreement awarded.

Legal Bases:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);
- Article 5.1 (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject);

- Article 5.1 (c) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract).

9. * Description of the category(ies) of data subject(s):

Data subjects are: the tenderer/applicant and partners and affiliated entities, subcontractors and their staff (both natural and legal persons).

10. When and how were data subjects informed:

The Privacy statement is made available on the CPVO website.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data processed are generally the following:

a) identification data:
- name (first name, surname, previous surname);
- gender, nationality, place and date of birth;
- passport number and ID number;
- signature of person or authorised representative;
- title, position, functions, department and company;
- contact details (website and email address, fax, business and mobile telephone number, official postal address, country of residence);

b) personal data contained in certificates for social security contributions and taxes paid, extracts from judicial records;

c) bank account reference (IBAN and BIC codes), VAT number, national insurance number;

d) A declaration of absence of conflict of interest;

e) Documents for the evaluation of selection criteria or eligibility criteria (expertise, technical skills and languages, educational background, professional experience including details on current and past employment);

f) A financial identification composed of the name, first name, address and contact details of the natural person owning the account. Should the natural person represent a moral person, he or she should identify the company for which the tenderer works. Same issue if the owner of the account is different from the tenderer;

g) Proof of security clearance and declaration of honour that they are not in one of the exclusion situations and/or administrative sanctions referred to in Article 136 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012, hereinafter Regulation 2018/1046.

For procurement procedures involving contracts worth more than EUR 144 000, the following data will be published in supplement S of the Official Journal of the European Union and on the website of the Office: name of the contractor, subject matter of the contract, amount legally committed.

For grant procedures: a) the name of the beneficiary; b) the locality of the beneficiary, namely: i. the address of the recipient when the beneficiary is a legal person; ii. the region on NUTS 2 level when the beneficiary is a natural person; c) the amount legally committed; d) the nature and purpose of the grant.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has also the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written

request to the CPVO data controller, Head of Legal service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

The right to rectification could be restricted after the time limit for receipt of requests to participate or tenders has expired, as per Article 169 of Regulation 2018/1046.

13. Storage media of data:

As regards electronic copies of documents containing personal data, these are stored in the internal database Docman. Physical copies of documents containing personal data are stored within locked cupboards within the public procurement sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- CPVO staff members in the Legal, Procurement and Logistics service;
- CPVO staff members in the Accounting and Finance sector;
- Concerned staff members in other Unit/services.

External recipients:

Some personal data is also disclosed to the public in order to meet the obligation to publish information on the outcome of procurement and grant procedures.

Upon request, data may be transferred to the legal advisors of the Office, the European Court of Auditors, the European Anti-Fraud Office (OLAF), the Internal Audit Service of the Office and the Court of Justice. The data transferred is limited to that strictly necessary for managing the procurement and/or grant procedures, or for official investigations or audits.

15. * Period of retention for the data:

In accordance with the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members, data relating to unselected candidates to a call for a tender/grant procedure, data will be destroyed after a period of twenty-four months from the date of the decision of the Office appointing the succeful candidate. Regarding successful candidates, the data will be at least retained during the whole period of validity of the concerned contract signed.

In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

As regards technical, strategical and other data which may render a tenderer identifiable, these cannot be disclosed without a prior review and decision of the CPVO authorities. CPVO staff members dealing with personal data in the management of log files must sign a confidentiality declaration and/or non-disclosure agreement.

As regards electronic storage of documents Docman, the database can only be accessed by CPVO/users from the internal network on premises or through the remote connection VPN SSL. The database is also username and password protected and access to the relevant document may be restricted to selected recipients.

Personal data collected are treated confidentially and processed solely by authorised staff members dealing with procurement, including staff dealing with financial matters and members of the opening and evaluation committees, exclusively for management and administration purposes. If applicable, external

experts and contractors assisting the Office with evaluations may be granted access to personal data on a *need-to-know* basis after signing a Declaration of confidentiality and of absence of conflict of interests. Data related to financial processing is further secured through an accounting software.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Internal Audits

2. * Last update of this record:

29/03/2021

3. Reference Number:

No 48

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal Auditor of the CPVO

7. Description of the processing operation:

Internal audits are carried out to advise the CPVO on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management. The activities carried out by the internal auditor involve assessing the suitability and effectiveness of internal management systems and the performance of the Office in implementing policies, programmes and actions, the efficiency and effectiveness of risk management, control and governance processes.

The CPVO has concluded a Memorandum of Understanding (MoU) with the EUIPO to share their Internal Audit capacity to perform those internal audits, which are coordinated internally by the Internal Control Coordinator of the CPVO.

Within the framework of internal audits, the internal auditor interviews staff responsible for these operations, carries out surveys, analyses documentation (internal guidance, etc.) and transactions in information systems and assesses the operation of the internal controls put in place by management in respect of these operations. To this end, the internal auditor may collect personal data to conduct assurance and consulting activities. The internal auditor enjoys complete independence and unlimited access to all relevant information required in the conduct of its activities in relation to all the activities and units of the CPVO. The audit process may imply sending documentation to the internal auditor.

Before an audit starts, information about the data subjects is collected, mainly from the CPVO organisation chart. The information is used for any further communications between internal audit and the audited area. Personal data may be also obtained during audit activities through interviews, or from documents analysed in the course of the engagements (minutes of meetings, transactions in information systems, operational instructions given by or on behalf of the auditee or other types of data specific to the engagement, etc.). The reports issued to the Management are anonymised; therefore, no data transfer must be considered.

Each year, the internal auditor proposes an annual audit plan to the President of the CPVO. During the audit, staff members are informed that they may be interviewed by the internal auditor, and that their

inputs may be gathered within the audit report. The internal auditor sends an announcement letter and a data protection privacy statement at the beginning of the audit, informing that in advance that the auditor may collect personal data in accordance with Regulation (EU) No 2018/1725.

The main auditees receive a first version of the report to check for correctness/completeness.

A draft report is sent to the CPVO Internal Control Coordinator and the Head of Unit concerned by the audit for official comments. The report contains recommendations for the CPVO units' activities (no staff member is mentioned directly as the audits concern globally the processes).

The final draft report is sent to the President, the Vice-President and the Heads of Unit (the reports sent to the Management are anonymised).

The final audit report is made available online on the Intranet of the Office, Sharepoint, only to few recipients, including the Head of the Administration Unit, the Internal Control Coordinator and the Accountant. It is also made available in Docman with limited access. The recommendations are introduced in a database for monitoring of the follow-up.

The CPVO then prepares an action plan detailing the corrective actions that will be implemented in response to the recommendations, their timing and the responsible person for the implementation. After completion of the period of implementation of the action plan, the internal auditor carries out a follow-up and issues a follow-up report.

8. * Purpose(s) of the processing and Legal Basis:

The processing of data is necessary for enabling the conducting of internal audits of the activities of the CPVO, for which access to data by the internal auditor is required. Internal audits do not typically target natural persons as such, yet, throughout the course of internal audits, personal data may be processed.

Legal instruments:

- Article 111 of Council Regulation No 2100/94 on Community plant variety rights;
- Memorandum of Understanding between the EUIPO and CPVO;
- Articles 78-80 of the CPVO Financial regulation;
- Internal Audit Charter.

Legal basis:

Article 5.1 (a) of Regulation (EC) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority);
Article 5.1 (b) of Regulation (EC) No 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members involved in internal audits.

10. When and how were data subjects informed:

The Privacy Statement is made available to the data subjects before the collection of personal data via email. It is also accessible in the intranet of the Office, SharePoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Potentially all data within the remit of the Office (paper and electronic records, databases) as well as recording interviews with staff at all levels, for which the following personal data is processed:

- Name and Surname;

- Title;

- Position, functions, Units/services or sectors in which the data subject works;

- Company contact details (internet, e-mail address, business telephone number, postal address).

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

All personal data related to the internal audit is stored in secure IT applications according to the Office's security standards. Data is stored in the CPVO's archiving system, Docman, and on the Internal Control coordinator's computer, which is password-secured. It is also stored on the Intranet of the Office, Sharepoint, in a folder with restricted access. Paper files are kept locked in locked cupboards.

In EUIPO, electronic documents are kept in the internal auditor's document management tool ShareDox and/or LimeSurvey (in case surveys are carried out as part of the audit), to which only internal auditing staff have access, as well as in Microsoft Outlook (where mail communications have been exchanged between the internal audit and the auditees). Paper files are stored in locked cupboards.

14. The recipients or categories of recipients to whom the data might be disclosed:

- Internal Auditor;
- Internal Control Coordinator of the CPVO;
- The Head of the Administration Unit;
- The Head of Unit of the CPVO Unit/Service concerned by the audit;
- The President and the Vice-President of the CPVO;
- The Administrative Council of the CPVO receives each year a summary of the audit report;
- Upon request, the Administrative Council can receive the full report;
- The EU Court of Auditors (access to the full report).

15. * Period of retention for the data:

In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal process.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Appropriate technical and organisational measures are in place to safeguard personal data collected throughout the course of internal audits.

In the CPVO, audit reports are stored within the Administration Unit. Electronic copies may be stored in the computer of the Internal Auditor, of the CPVO Internal Control Coordinator, of the President and Vice-President of the Office and of the Heads of Unit concerned, as well as in the internal database Docman, which is password-secured. Some documents may be uploaded on the Intranet of the Office, SharePoint, under a restricted access on a *need-to-know* basis. As to e-mail exchanges in the CPVO's Outlook Webmail, these are well duly secured.

In the EUIPO, all personal data related to the internal audit is stored in secure IT applications according to the Office's security standards. Data may be stored in EUIPO's document management tool, as well as

in Microsoft Outlook for correspondence management. The security standards for the Information Security Management System are based on ISO 27001. All persons dealing with personal data in the context of the IT systems, at any stage, have signed a confidentiality declaration and/or non-disclosure agreement.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Research and Development Projects

2. * Last update of this record:

18/03/2021

3. Reference Number:

No 49

4. * Name and contact details of the Controller:

Head of Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Technical Unit

External processor:

Entrusted Examination Offices

7. Description of the processing operation:

R&D proposals can be submitted to the CPVO via e-mail for financial aid and other types of support. Submissions can be lodged by Examination Offices, research institutions, universities, breeder organisations and individuals. Applications for financing should include: a short description of the project, its relevance for the CPVR system, the state of the art of the techniques in question, follow-up actions and an estimate of the costs. A template is used for the application and includes a collection of personal data of the Applicants such as full name, contact information, organisational affiliation and position.

In some cases, institutions and bodies from third countries may join a given project, in which case, they generally take care of the financing the research project, unless co-funding is agreed. The same categories of data as the ones required for R&D proposals coming from within the EU is here required.

Upon receipt of the proposal at hand, the technical expert (Case Holder/CH) of the CPVO examines the proposal and checks if the application contains the necessary information about the project for its assessment. The CH also evaluates if the project is in line with the CPVO R&D strategy. The CH might involve further CPVO colleagues in this analysis.

Depending on the CH's analysis, a project proposal may be refused, made subject to a request for further clarification, or considered to be ready for further processing. If the CH's analysis is positive, the project evaluation is launched, and an external expert group is asked to provide an opinion. Based on the CH's analysis and the expert group opinion, the R&D advisory group will prepare a proposal to the President for decision on co-funding.

If an application is accepted and once the decision of the President has been signed, the Head of the Technical Unit sends by email, a request to the Procurement Sector requesting for the financial commitment to be made with all relevant documentation supporting the request (application, any opinions and the decision of the President).

Upon finalization of the Contract, the Head of the Technical Unit sends it to the parties for signature. The signed contract is a precondition for the start of the project. Within the framework of the contract, an interim report and a final report of the project are generally issued.

8. * Purpose(s) of the processing and legal basis:

The processing is necessary to enable the evaluation of R&D proposals submitted to the CPVO, for the CPVO to decide in turn on co-financing of R&D projects.

Legal Instruments:

- CPVO Administrative procedure of 2 December 2020 for Co-financing of R&D projects;
- Rules of the Administrative Council of the CPVO of 19 September 2019 on R&D;
- Contractual Arrangements between the CPVO and the concerned Body/Institution(s).

Legal Bases:

Depending on the case and specific Contractual Arrangement signed between the CPVO and the concerned Body/Institution(s), the following legal bases apply:

- Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority);

- Article 5.1 (c) of Regulation 2018/1725 (processing is necessary for the performance of a contract);

- Article 5.1 (d) of Regulation 2018/1725 (the data subject has given consent to the processing for one or more specific purposes).

9. * Description of the category(ies) of data subject(s):

Experts from entrusted Examination Offices, experts from the breeding industry and experts from research institutions, universities or other testing centres.

10. When and how were data subjects informed:

The Privacy Statement is made available to the data subject together with the application form.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Name and Surname;
- Title;
- Contact details (postal address, e-mail address);
- Name or organisation of affiliation;
- Type of affiliation (position).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Technical Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Personal data are stored in electronic format in the intranet of the Office, Sharepoint, and in the Contacts database. For more information on Contacts database, please refer to Record No 43 Contacts Database.

14. The recipients or categories of recipients to whom the data might be disclosed:

The data is disclosed on a *need-to-know* basis to staff members of the Technical Unit, the Administration Unit, the Legal service, and the Presidency, Vice-President and Senior Advisor of the Office.

The final report of the project is published on the CPVO website, thus, it is made available to the public at large.

15. * Period of retention for the data:

Personal data within the framework of Research and Development Proposals stored in the intranet of the Office, Sharepoint, and in the Contacts database are kept as long as required for the fulfilment of the implementation of the contractual arrangement concerning the specific project. Once the data is no longer deemed necessary, it is accordingly deleted.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

It is possible (for an Examination Office for instance, acting as coordinator of a cofounded R&D project with the Office) to involve an institution located in a third country outside of the EU in some R&D projects, context where personal data may be exchanged and processed. In case a third country institution is involved, the CPVO carries out *ex ante* a due diligence exercise taking into consideration the consequences of such potential transfer of data and ensuring that the appropriate safeguards are put in place.

If such a transfer of data is deemed acceptable within the framework of the project and access to personal data of the data subjects is granted, this access will at any rate be temporary and only until the end of the research assignment. This transfer of personal data will be made based on a mutually agreeable contractual arrangement for a fixed period limited to the duration of the research project.

17. * Measures to ensure security of processing:

Access to the data stored is granted only to authorised members of the staff. The Office takes a number of technical and organisational measures to prevent unauthorised disclosure.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), please see the privacy statement.

[i] The fields marked with (*) are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Opening of Bank Accounts on behalf of the CPVO and Corporate Credit Cards

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 50

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu.

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu.

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Accounting and Finance sector)

External processors:

Caisse d'Epargne, Crédit Agricole, LCL Banque et Assurance, BNP Paribas, Société Générale, Crédit Mutuel Arkéa, Lufthansa AirPlus Servicekarten GmbH.

7. Description of the processing operation:

The CPVO enters into agreements with different banks in order to be able to process the relevant payments and financial commitments necessary to perform its functions. The Office, as European Union agency, has also the possibility to invest on financial products or open an imprest account.

Where the CPVO opens a bank account, certain categories of personal data are requested from the President of the CPVO, his delegates (Vice President and Heads of Units) and the staff allowed to sign banking orders or to consult data though electronic services. The Administration Unit collects the data, which is then sent to the bank in order to establish, renew or modify the contract. Likewise, in order to issue and receive all the necessary payments related to the functioning of the Office, personal data are processed.

In addition to this processing, the CPVO has reached an agreement with a financial organisation, namely, Lufthansa AirPlus Servicekarten GmbH, for the supply of corporate credit cards for the staff of the Office. The credit card is intended to be used primarily to pay costs related to missions undertaken by staff on behalf of the Office. It also allows for payment of medical expenses while waiting reimburserment from the Institutions. The Staff member can apply for a credit card by contacting the Administration Unit which has the sole authority to make requests for a card on behalf of staff. The Accountant or Deputy Accountant posts the hard copy of the application for the credit card to the financial organisation providing the cards. No copies are kept by the Accountant or Deputy Accountant. Only a notification is sent to the Human Resources sector, which states that a Staff member possesses a credit card. This notification is kept in the secured Personal file.

8. * Purpose(s) of the processing and legal basis:

The purpose of processing is to carry out all the relevant financial activites necessary to the functioning of the Office. The processing is also necessary to establish banking details of the financial transactions such as the identification of the person responsible for the banking action or the request.

Legal instruments:

- CPVO Financial Regulation;
- Article 30 of Council Regulation (EC) No 2100/94 (legal personality of the CPVO);
- Contracts signed with the Banks;
- CPVO Credit card procedure of 30 November 2009.

Legal Basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

- Staff members acting as authorised officials and the accountancy team, to sign banking orders;
- All the Staff members of the CPVO;
- Every CPVO staff members willing to possess a Corporate credit card;
- Natural persons paying fees or receiving payments by the CPVO;
- Suppliers of the CPVO.

10. When and how were data subjects informed:

The personal data are processed during the establishment of the contracts and when concerned job holders take up or change post in the CPVO. The contracts signed with financial institutions include notices on the relevant national legal framework applicable and further information on the processing of data. The notice is made available on the intranet of the Office, Sharepoint.

The Privacy Statement is also made available to CPVO staff members in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data vary in relation to the use made by the CPVO for the banks, in particular:

Crédit Agricole processes the following data:
- Name, surname, email address and banking information of all the CPVO staff (including the person in charge for internal control);
- Corporate account information;
- Name, surname, email address, banking information, signature, place of birth, birthdate and phone number of the responsible person within the accountancy team (part of the Administration Unit) as well as authorising officers;
- Name, surname, email address and banking information of natural persons paying fees or receiving payments from the CPVO;
- Name, surname and email address of the staff member in charge of the internal control;
- CPVO suppliers' necessary data to process the payments, including the name and surname of the recipients (when applicable), postal and/or e-mail address (where applicable) and banking information;

LCL, Crédit Mutuel Arkéa, Caisse D'Epargne and BNP Paribas process the following data:
- Name, surname, email address, banking information, signature, place of birth, birthdate, ID photo and phone number of the responsible person within the Accountancy sector (part of the Administration Unit) as well as of authorising officers;
- Corporate account information;
- Name, surname and email address of the CPVO staff member in charge of the internal control (only Caisse D'Epargne)
- CPVO suppliers' contact information;

Lufthansa AirPlus Servicekarten GmbH process the following data:

- Name of the employer, name, address, staff ID of the CPVO Staff Member willing to possess the corporate Credit Card;
- Additional information received by the Travel Service Provider as cost center, airline ticket number and car rental details (if applicable).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No. 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Personal data contained in the notification regarding the issuance of the corporate credit card are stored within the personal files of the staff member. Original copies of the contract signed with the banks are kept within the Accountancy offices. Further documents in digital format are kept within the internal database Docman.

Data are also stored in the servers of external processors and their sub-processors, in the European Union. However, in some cases data may be transferred outside the EU (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- Staff members within the Administration Unit allowed to sign banking orders, in particular within the Human Resources sector and the Accounting and Finance sector. They also act as recipients for corporate card requests. In this respect, AirPlus transfer credit card holder's data (such as data related to transactions made by the employee) to the person in charge of the issuance of corporate card.

External recipients:

- LCL: Data might be disclosed to affiliates within the Groupe Crédit Agricole, administrative authorities, sub-processors, LCL partners and intermediaries;
- BNP Paribas : Data might be disclosed to affiliates within the Groupe BNP Paribas as well as other entities outside the Groupe as service providers, administrative authorities and partners;
- Caisse d'Eparagne: Data might be disclosed to entities belonging to the the Groupe BPCE, BPCE's partners, sub-processors of the Caisse D'Eparagne; in specific cases, data might be disclosed to administrative and financial authorities.
- Arkea Credit Mutuel: Data may be disclosed to its sub-processors; in specific cases, data might be disclosed to administrative and financial authorities;
- Société Général: Data might be disclosed to affiliates within the Groupe Société Générale, partners and sub-processors; in specific cases, data might be disclosed to administrative and financial authorities;
- Lufthansa AirPlus Servicekarten GmbH: Under strict rules of confidentiality, data may be disclosed to the following categories of service providers: IT service provides (hosting and infrastructural services), transaction-related service providers and Customer relationship service providers (call center services); all the service providers are located in the EU; in specific cases, data might be disclosed to administrative and financial authorities.

15. * Period of retention for the data:

Concerning the documents kept at the Office, accordingly with the Financial Regulation, documents, either physical or on electronic format on Docman, are deleted and destroyed after a legal retention of 7 years starting on the date of the termination of the contract.

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, personal data contained in the notification regarding the issuance of the corporate credit card are destroyed after a period of 10 years from the date of the end of contract of the staff member.

As for external processors, data is retained for the longer of the period required in order to comply with applicable laws and regulations or another period regarding operational requirements, as account

maintenance, facilitating client relationship management, responding to legal claims and/or regulatory requests. In particular, the retention period adopted by Caisse D'Epargne, LCL and BNP Paribas is ten years from the end of the relationship (closing account). Caisse D'Epargne also applies a shorter retention period when data are processed for the management of specific products and services. Finally, the retention period of Société Général is set at 5 years after the end of the business relationship. The retention period may vary in relation to the specific financial service provided by the external processors.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The following banks do not transfer data outside the EU/EEA:
- LCL;
- Crédit Mutuel Arkea;

The following processors might transfer data outside the EU/EEA:

- BNP Paribas. Transfers are governed by Adequacy decisions of the Commission (when applicable); derogations, as in the case of execution of a contract (i.e. execution of an international payment), Standard Contractual clauses approved by the Commission as well as Binding Corporate Rules.

- Société Général. It transfers data to two affiliates of the Group Société Général, located respectively in Romania and India. The purpose of the transfer is to comply with Code Monétaire et Financier (L. 561-4-1), requiring the bank to verify the identity, suitability and risks involved with maintaining a business relationship (also known as KYC- Know Your Customer). Transfers are governed by Standard Contractual Clauses approved by the Commission.

17. * Measures to ensure security of processing:

Personal data is stored in the internal database Docman according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. As an additional layer of security, Docman may only be accessed by CPVO/users from the internal network (on premises) or through the remote VPN SSL. Access is restricted only on the need to know basis tothe Accountant or Deputy Accountant, Human Resources sector and IT System Administrators.

Contracts with financial institutions are physically stored in locked cupboards, accessible only to the Acounting and Finance staff members.As regards personal files of staff members, these are only accessible by Human Resources staff members and the staff member concerned.

The relevant financial flow exchange between financial institutions and the CPVO is further encrypted through a secure IT tool to safeguard the data processed.

The external processors take all the necessary precautionary measures to preserve the security of personal data from being distorted, damaged, made inaccessible or from being accessed by unauthorised third parties. Both Arkea Crédit Mutuel and Caisse D'Epargne also adopted the necessary organisational measures, through training of teams dedicated to the issue of information security. Still, when coming into agreement with sub-processors, Arkea and Caisse D'Epargne chose sub-contractors or service providers who offer a high level of guarantees regarding the implemebtation of appropriate technical and organizational measures. Moreover, Caisse D'Epargne carry out internal audits in order to guarantee the effective level of data protection.

The Controller monitors the implementation of Regulation (EU) 2018/1725 as regards the organisational and technical security measures adopted by the sub-processors.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Insurance coverage of CPVO staff and Third persons

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 51

4. * Name and contact details of the Controller:

Head of Administration
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processors:

Administration Unit (Human Resources sector)
Legal, Procurement and Logistics service

External processors:

MMA (professional civil liability insurance, covering both staff members and external visitors)
CIGNA (missions insurance) (within European Commission's Framework Contract)

7. Description of the processing operation:

In order to protect its staff inside and outside the CPVO premises, the Office enters into contracts with insurance companies. An insurance policy also covers the visitors of the CPVO when they are inside the Office premises.

The insurances cover the following elements:
- As regards the civil liability for the staff, trainees, national experts, as well as external visitors and other third parties, the CPVO signed contracts with the insurance company MMA. This insurance policy protects third persons within CPVO premises.
- As regards missions, the CPVO uses the framework contract of the European Commission's framework contract with the company CIGNA. This company is specialized in insuring travelling persons, for business or leisure purposes. The insurance policy under CIGNA protects the staff members on mission outside the CPVO. The CPVO indicates each year how many missions were performed in the previous year to adapt the amounts of coverage by this specific insurance.

Each time the insurance contract is renewed the CPVO indicates to the insurance company the quantity of staff members concerned.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is to enable the CPVO to conclude contracts with insurance companies to ensure that CPVO officials in active employment are accorded working conditions that are compliant with appropriate health and safety standards, as well as to to cover third parties at the CPVO premises.

Legal instruments:

- Article 1e (2) of the Staff Regulations of Officials;
- CPVO Financial Regulation.

Legal basis:

- Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO Staff members and third parties visiting the CPVO premises.

10. When and how were the data subjects informed:

At the time of the signature of an employment contract with the CPVO, the new staff member is informed about the insurances which will cover his/her professional activities and duties. Staff members to be sent on mission outside the CPVO premises are also informed on the coverage by an insurance. The CPVO staff members have as well a Privacy Statement available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Only in those cases of an insurance claim, data related to the identity of the staff member is transferred to the insurance companies. Data transferred are name, surname and position held within the CPVO. No other data is transmitted to the insurance companies.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The Data Subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Electronic personal files are stored in Docman (electronic storage of documents). Data are stored in servers located within the CPVO premises. The data in paper is stored under locked cupboards accessed by Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Administration Unit (Human Resources sector)
Legal, Procurement and Logistics service

External recipients:

MMA (professional civil liability insurance, covering both staff members and external visitors)
CIGNA (within European Commission's Framework Contract)

Data may be disclosed to sub-processors for the purpose of providing the service.

15. * Period of retention for the data:

In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations. However, the sub-processor Cigna may transfer personal data outside the EU. International transfers may be triggered only on reactive or on demand basis in order to respond to specific requests of the data subject, under the condition that the data subject has already put forward an insurance claim. The location of the transfer may vary in relation to the Service Center capable of satisfying the request of the data subject.

Transfers are governed by Data Transfer Agreements containing Standard Contractual Clauses adopted by the Commission.

17. * Measures to ensure security of processing:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

Data are transferred to the external service provider only in cases of insurance claims. The insurance companies receives only the amount of data subject to be insured.

The contracts concluded with the insurance companies are duly stored and secured by Human Resources sector and the Legal, Procurement and Logistics sector in the CPVO database Docman. A clause of confidentiality is also included in the contracts concluded with the insurance companies.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Business Continuity Plan

2. * Last update of this record:

14/04/2021

3. Reference Number:

No 52

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit

External processors:

Broadcom and its sub-processors

7. Description of the processing operation:

This processing concerns the implementation of the Business Continuity Plan (BCP) of the CPVO in the event of crisis. The BCP has been designed as a practical guide for CPVO staff members and serves to outline all necessary measures to be triggered to respond efficiently to a crisis and to ensure delivery of essential tasks by the Office. A crisis is defined as any event or disruption that could impact the image of the system, the basis of the organization and the CPVO staff. The BCP envisages the arise of two types of crisis:

- Predictable crisis (e.g.: major strike, disease outbreak, etc.): where there is sufficient warning to implement a pre-planned strategy.

- Sudden crisis (e.g.: IT system failure, power failure, flood, earthquake, terrorist attack, hijacking): where there are little or no signals, and a pre-identified programme to deliver key tasks will need to be implemented.

During a crisis, all staff members will be contacted on their office phone numbers via Dialog Connect. This is a unified communication tool that enables CPVO staff members to have an additional communication tool to guarantee the smooth functioning of the Office in case of crisis. Staff members are required to install the application on their private mobile phones.

The Communication Officer will send out a mass message informing staff about the crisis and the measures to be taken. Members of the Administrative Council of the CPVO will be contacted via professional phone numbers or e-mail addresses.

In the case of absence of the Communication Officer, it is the Head of the Technical Unit who will carry out these communication tasks. The other members of the crisis management team can have access to the list of numbers in case of absence of both.

8. * Purpose(s) of the processing and legal basis:

The processing of personal data is necessary for the implementation of the Business Continuity Plan (BCP) of the Office in cases of crisis, to manage risks for the smooth running of the Office, ensuring that it can continue to deliver its key tasks and responsibilities in the event of major disruption. It covers both the crisis response and the recovery arrangements with respect to disruptions.

Legal instruments:

- CPVO Procedure of 31 March 2019 on CPVO IT Standards and IT Test Security Plan;
- Business Continuity Plan of the CPVO.

Legal Basis:

Article 5(1)(a) of the Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members, Seconded National Experts, Interim Agents, Trainees, and members of the Administrative Council of the CPVO.

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint under the Data Protection Officer section.

The President of the CPVO will ensure that staff covered by this Plan are given effective, regular, training, and the necessary administrative support to allow them to carry out their functions. The BCP will be regularly up-dated and maintained by the staff member responsible for Internal Audit and Control. Updates will be posted on Sharepoint as they occur.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Data collected from staff members:

- Name and Surname;
- Replacing staff (only initials are processed);
- Professional email address.

Data collected from Administrative Council members:

- Name and Surname;
- Professional e-mail address;
- Professional phone number.

Additional connection data may be gathered by the external service provider.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict processing, to erase, to object etc,):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The personal data of all CPVO staff members and members of the Administrative Council of the CPVO are kept respectively in Appendix 3 and Appendix 1 of the CPVO Business Continuity Plan. The BCP is stored

in the Intranet of the Office, Sharepoint, and in the professional device of the Internal Audit and Control Coordinator, responsible for updating the BCP.

Regarding the external service provider, data are stored within internal servers of the sub-processor within the EU. However, additional data may be available to sub-processors outside the EU for the purpose of providing the service (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Personal data may be accessed by those directly involved in the decision making and management of a crisis as well as the external processors on a *need-to-know* basis, in particular:

Internal recipients:

- Crisis management team leader: President of the CPVO and substitute (Vice-President);
- Coordinator: Head of Administration and substitutes (Head of the Technical Unit and Senior Adviser);
- Communication: Communication Officer and substitute (Head of the Technical Unit);
- Log book: Assistant to the Presidency and substitute (Head of the Technical Unit);
- Technical Unit: Head of the Technical Unit and substitute (Deputy Head of the Technical Unit).

External recipients:

- Broadcom and its sub-processors for providing the service.

15. * Period of retention for the data:

According to the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of the CPVO staff members, personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

Regarding personal data related to the Administrative Council members, it will be kept for the duration of their mandate. For traceability reasons and particularly audit purposes, the records may be kept for further 2 years.

As regards data processed by the sub-processor, data is retained as long as necessary to provide the service, in accordance with the purposes of processing.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

In principle, personal data is not intended to be transferred to a third country or international organization. As regards the external processors, however, in specific circumstances additional personal data may be transferred for the purpose of providing the service. These transfers should be governed by Binding Corporate Rules approved by the European Commission and APEC Privacy Certification module.

17. * Measures to ensure security of processing:

Contact details of all staff members are reported in Appendix 3 of the CPVO Business Continuity Plan, which is held by the Internal Audit and Control Coordinator on his/her professional device. The contact details of the Administrative Council members are held in the Appendix 1 of the CPVO Business Continuity Plan, which is retrieved from the internal tool Tableau. For more information on the security measures in Tableau, please refer to Record No 70 Tableau.

The BCP is also available in the intranet of the Office, Sharepoint, and access is restricted to authorised members. Sharepoint may only be accessed by CPVO/users from the internal network or through the remote connection VPN SSL.

As regard the external processors, the Controller monitors the implementation of the Regulation (EU) 2018/1725 concerning the security measures adopted by its sub-processors.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Management of Requests for Leaves and Absences

2. * Last update of this record:

08/04/2021

3. Reference Number:

No 53

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human resources sector)

External processors:

- DG HR European Commission
- SYSPER 2 European Commission
- DG DIGIT European Commission
- PayMaster Office (PMO) (European Commission)

7. Description of the processing operation:

The processing operation concerns the management of requests for leaves and absences of CPVO staff members. This operation takes place under the TIM module of SYSPER, the module relating to Time Management. SYSPER is a software created and managed by the European Commission, of which the CPVO makes use, which requires the processing of personal data in connection with the personal file of each staff member. For more information on SYSPER, please refer to Record No 68 SYSPER.

The specific TIM sub-module includes the following types of requests for leaves and absences:
- Annual leave;
- Recuperation;
- Special leave;
- Compensation;
- Sick leave;
- Other absence.

For each request for leave or absence, SYSPER makes use of the necessary data contained in staff members' personal file, including entitlements, annual rights, place of origin, work pattern, age, family composition, and private address. In all cases, the staff member needs to indicate the type of leave and select the period of time for the absence, as well as further specific data in the case of some types of leave. For instance, in the case of sick leave, a medical certificate must be lodged. Some further non-

mandatory fields are available (Reason for leave, Address, telephone number, comments). If no specific address is introduced, the private address of the staff member is taken by default. If an address different from the private address is introduced, a specific request should then be send to the Appointing Authority.

SYSPER displays the authorised number of days and travelling time allowed. For some types of leaves, once the staff member introduces and validates the request, a message appears demanding the provision of the supporting documents justifying the leave. After having sent the leave request for validation, the line manager of the staff member (Head of Unit/Sector) receives a notification to validate the request for leave. The line manager then reviews and signs, if appropriate, the leave request. Further, the Human Resources sector has the possibility to view all specific requests to check the presence or absence of the expected supporting documents.

8. * Purpose(s) of the processing and legal basis:

The processing is necessary for the management of leaves and absences of CPVO staff members.

Legal Instruments:

- Commission Decision of 16 December 2016 on leave;
- Decision of the Administrative Council of the CPVO of 16 March 2020: Adoption by Analogy of Commission Decision C(2020) 1559 on leave;
- Articles 15, 35, 40, 42, 42a, 42b, 42c, 57, 58, 59, 59a, and 60 of the Staff Regulations of Officials.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members (Officials, Temporary Agents, Contract Agents), Seconded National Experts, and Trainees.

10. When and how were data subjects informed:

The Privacy Statement is made available to the data subjects in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following categories of data are processed:

- Staff member personal number, name, first name, civil status, nationality, date and place of birth, grade, service, career history, family composition, private address;

Depending on the type of leave/absence concerned, further data may be required to be processed. For instance, in the case of requests for sick leave, medical certificates justifying the request are needed.

For more information, please refer to Record No 68 SYSPER.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, the Head of Administration Unit, at dpc@cpvo.europa.eu by *explicitly* specifying *the request.* The CPVO has put in place an Internal Procedure to be followed by the CPVO Controllers in relation to Rights exercised by data subjects in accordance with Regulation 2018/1725 dated 20 March 2021.

13. Storage media of data:

Please refer to Record No 68 SYSPER.

14. The recipients or categories of recipients to whom the data might be disclosed:

Access to the personal data processed is granted on a *need-to-know* basis.

Internal recipients:

- Staff member concerned;
- Administration Unit (Human Resources sector);
- CPVO Heads of Units/Signing Authority (line manager).

External recipients:

- DG HR European Commission
- SYSPER 2 European Commission
- DG DIGIT European Commission
- PayMaster Office (PMO) (European Commission)

15. * Period of retention for the data:

Please refer to Record No 68 SYSPER.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no transfers of data foreseen to third countries or international organizations.

17. * Measures to ensure security of processing:

The measures put in place to ensure the security of the present processing are those concerning SYSPER. For more information, please refer to Record No 68 SYSPER.

Where the requests for leaves and absences require justifying documents for approval of such (e.g.: medical certificates when requesting a sick leave), these are only stored in SYSPER and access is restricted to the staff member concerned and authorised staff members of the Human Resources sector.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Appointment of Qualified members of the Board of Appeal of the CPVO

2. * Last update of this record:

23/03/2020

3. Reference Number:

No 54

4. * Name and contact details of the Controller:

Head of the Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal service

7. Description of the processing operation:

The processing operation concerns the appointment procedure of the Qualified Members of the Board of Appeal of the CPVO, for which several categories of data must be processed. The Board of Appeal of the CPVO is the body responsible for deciding on appeals against decisions of the Office.

Regarding the appointment procedure of the Qualified Members of the Board of Appeal of the CPVO, it is opened with the publication of a call for expression is published in the Official Journal of the European Union (as well as with the corresponding announcement on the CPVO website). The President of the CPVO then sets-up a Selection Panel for the selection process. The candidates must send an application with a CV and a declaration of independence to the Registrar of the Board of Appeal. The Selection Panel then sends an invitation for an interview to approximately twenty candidates with the best professional profiles, selected on the basis of their merits and the criteria set in the call for expression.

Following the interview, the President of the CPVO adopts a short-list of candidates which is presented to the Administrative Council for adoption. The selected members of the Board of Appeal are appointed for a period of five years (the term of office is renewable).

The CPVO is also in charge of the remuneration for the provision of services as Chaiperson, Alternate Chair, Rapporteur or Member of the Board of Appeal, as well as of the reimbursement of the expenses incurred by them during the performance of their duties.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is enabling the appointment of Qualified (legal or technical) members of the Board of Appeal of the CPVO and the payment the remuneration for the services provided as well as the reimbursement of the expenses incurred by them during the performance of their duties.

Legal Instruments:

- Articles 46, 47 and 48 of Council Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights;
- Article 11 of Commission Regulation (EC) No 874/2009 of 17 September 2009establishing implementing rules for the application of Council Regulation (EC) No 2100/94 as regards proceedings before the Community Plant Variety Office.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

External candidates to the position of qualified member of the BoA.

10. When and how were data subjects informed:

The candidates are provided with information concerning data protection in the call for expression of interest. Once appointed, the members of the Board are also provided with information concerning data proteccion in the payment request form for the remuneration of their services.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected:
- Name and Surname;
- Postal Address;
- E-mail address;
- Telephone number;
- Organisation/Member State;
- Current position;
- Legal and/or Technical field(s) of expertise;
- Relevant work experience (including trainings);
- Length of service;
- Language skills,
- Professional reference from an examination office or specialized legal office in intellectual property;
- CV;
- A written and signed declaration of independence and absence of conflict of interest;
- Bank account information: name and address of the bank, IBAN number, account number, swift code.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725. In order to access personal file in paper form or rectify, block, object and erase his/her personal data kept in personal file, data subject must submit a written request to the CPVO data controller, Head of Legal service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The applications CVs and declaration of interests are stored in the internal database Docman as well as on paper at the premises of the Registrar of the Board of Appeal in locked cupboards. Financial data are stored in the internal database EPM.

14. The recipients or categories of recipients to whom the data might be disclosed:

The CPVO President, the Selection Panel, the Registrar of the Board of Appeal of the CPVO, and the members of the Administrative Council of the CPVO.

15. * Period of retention for the data:

All working documents, in paper or electronic format, submitted to the CPVO within the framework of appointing the Members of the Board of Appeal of the CPVO are destroyed at the end of the appointment period (usually after 5 years). Personal data related to unsuccessful candidates are destroyed after a retention period of 24 months from the date of the decision of appointment by the Administrative Council of the CPVO.

Regarding financial data and supporting documents within the framework of reimbursement costs, in accordance with Article 42(5) of the CPVO Financial Regulation and Article 21(d) of its Implementing Rules, these data are kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organizations.

17. * Measures to ensure security of processing:

The physical personal files are locked in a cupboard accesed by the Registrar of the Board of Appeal of the CPVO. Access to electronic personal files within Docman is username- and password-secured and can be accessed only by the Registrar of the Board of Appeal of the CPVO and the IT Administrators on a *need-to-know* basis.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Designation of Confidential Counsellors and Procedure for Harassment cases at the CPVO

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 55

4. * Name and contact details of the Controller:

Head of the Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of processor:

a) Designation of Confidential Counsellors within the CPVO:

- Head of Administration Unit;
- Members of Selection Panel (appointed staff members of the Human Resources sector and of the Staff Committee).

b) Procedure against Harassment within the CPVO:

- Head of Administration Unit;
- Confidential Counsellors;
- CPVO Medical Advisor, if applicable;
- Concerned Head of Unit/President, if applicable.

7. Description of the processing operation:

The processing operations consist in: a) the appointment by the CPVO (Selection Panel) of Confidential Counsellors; and b) enabling CPVO staff members allegedly suffering from harassment within the CPVO to report the case. To this end, the CPVO has introduced a common policy of prevention of psychological harassment and sexual harassment within the context of the Staff Regulations of Officials introduced an informal and formal procedure relating to psychological and sexual harassment, and committed to undertake appropriate action (if necessary, disciplinary measures) in accordance with the Staff Regulations of Officials against any person who is found guilty of psychological or sexual harassment at the end of a formal procedure. As an employer and to protect its staff, the CPVO must guarantee respect for the dignity of women and men at the workplace.

Confidential Counsellors, in their mission of hearing and mediation, handle personal data indirectly or directly related to the plaintif and the alleged accused person (the parties). Data may be collected by the Counsellors themselves during interviews.

a) Designation of Confidential Counsellors within the CPVO:

An internal call for application is held by the CPVO is order to nominate at least three Confidential Counsellors, containing the details of the position and the selection criteria of the appointment. The selection is done through an internal call for application. The staff members interested in the position must fill in and sign a dedicated application form along with a Statement of Honour. The application forms are then received by the CPVO Human Resources sector and subsequently presented to a Selection Panel consisting of representatives of the Human Resources sector and of the Staff Committee.

b) Informal Procedure on Harassment within the CPVO:

The informal procedure on harassment can be opened within the CPVO upon request of an alleged victim reporting the case. The alleged victim will contact the Confidential Counsellors, and the Coordinator (appointed staff member of Human Resources sector) will also be involved in the procedure.

During the Informal Procedure on the alleged harassment, Confidential Counsellors are entitled to listen, record, and summarise the core of the complaint and defense, process during which data issued from the parties may be copied, written and transmitted. This period of investigation implies the disclosure of very sensitive data (former experiences, judicial matters, health data, psychological evaluation).

Confidential Counsellors can also confront both parties to the procedure to gather both sides. Personal data can be eventually disclosed during the mediation period to each of the parties in order to recall the facts, and the Confidential Counsellors may record comments. However, at all stages of the procedure, Confidential Counsellors cannot take any step without the consent of the alleged viticm and that only anonymous data can be processed without a consent.

Finally, the alleged victim may decide to proceed to the Formal procedure. At this stage, results of the Informal procedure are sent to the Human Resources sector only responsible to call for a formal Investigation Panel and only if the victim consents to it.

8. * Purpose(s) of the processing and legal basis:

The purposes of the processing activities here described are to designate Confidential Counsellors and to manage the Informal Procedure for cases of harassment at CPVO.

Legal Instruments:

- Articles 12, 12a, 24 and 90 of the Staff Regulations of Officials;
- Articles 11, 46, 81 and 117 of the Conditions of Employment of Other Servants (CEOS);
- CPVO Decision on the CPVO policy of 11 May 2017 on protecting the dignity of the person and preventing psychological harassment and sexual harassment;
- Manual for CPVO informal procedures within the framework of the CPVO policy on protecting the dignity of the person and preventing psychological and sexual harassment;
- EDPS Guidelines of February 2011 concerning the processing of personal data during the selection of confidential counsellors and the informal procedures for cases of harassment in European institutions and bodies;
- Articles 1 and 31(1) of the EU Charter of Fundamental Rights.

Legal Basis:

For the alleged staff member accused of harassment:
- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

For the alleged victim of harassment:
- Article 5.1 (d) of Regulation (EU) 2018/1725 (the data subject has given consent to the processing of his or her personal data for one or more specific purposes).

In some instances where sensitive data may be processed, the following legal bases apply:
- Article 10.2 (a) of Regulation (EU) 2018/1725 (the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject);
- Article 10.2 (b) of Regulation (EU) 2018/1725 (the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

a) For the Designation of the Confidential Counsellors:

The staff member candidate to the Confidential Counsellor position, must fill in the application form in the context of the call for expression, for which the following data are required:

- Name and Surname;
- Current position; Unit/Service;
- Grade/Step;
- Date of taking up duties at the CPVO;
- Contact details (e-mail address);
- Candidates may also provide personal reasons of their application (e.g.: former experiences or trainings dealing with harassment cases).

b) For the Informal procedure:

Following the categories description (hard and soft) drafted within the EDPS Guidelines on harassment, the following different types of data which may be processed:

Hard data:

- Personal data related to the identity of the alleged harasser and victim (name and surname);
- Professional data related to the alleged harasser and victim (position at the Office).

Soft data:

- Reports and Comments of the Confidential Counsellors;
- Minutes from the investigation or interviews with both confronted parties or with witnesses;
- Potential revelations on Health data (or other sensitive data) by the victim.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

By default, data subject have the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.* However, for the processing here described, the following applies:

For the designation of Confidential Counsellors:

Upon request to the controller, data subjects have the right to access and update or correct their factual data, even after the deadline for submitting the applications. There is no possibility to update and correct data relating to merits and skills after the deadline for application.

For the Informal Procedure:

The rights to access, rectify, restrict, object and erase may be restricted by the controller in the procedures for cases of harassment in accordance with the Administrative Council Decision of 1 April 2020 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the CPVO.

13. Storage media of data:

a) For the designation of Confidential Counsellors:

- Physical copies are kept in locked cupboards at the premises of the Human Resources sector, and electronic copies are stored in the internal database Docman.

b) For the Informal procedure:

- Information from alleged victims may be received by email communication;
- Otherwise, all relevant documents produced and the data processed within the context of the Informal procedure must be kept physically, on paper. No electronic document shall be stored on the internal database Docman. Should an electronic document be needed in the context of the Informal procedure, such should be kept/sent in a duly secured disk.

Electronic listings of cases may be kept digitally, but in such case, they are anonimised.

14. The recipients or categories of recipients to whom the data might be disclosed:

a) Designation of Confidential Counsellors:

- Staff members in Human Resources sector/Head of Administration Unit;
- Appointed member of the Staff Committee in the Selection Panel;
- The President of the CPVO.

b) Informal procedure:

- Confidential Counsellors;
- Appointed Coordinator (staff member of the Human Resources sector);
- Where applicable, the Ombdusman.

15. * Period of retention for the data:

a) Retention policy for the designation of the Counsellors:

In accordance with the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members, the documents which are submitted during the designation procedure are destroyed after a period of retention of 24 months from the date of the appointment of the Confidential Counsellor. Regarding all working documents, in paper or electronic format, used by the members of the Selection Panel appointed for this recruitment procedure, these shall be destroyed once the selection procedure is closed, namely, on the date of the decision of the appointment of the Confidential Counsellor. Said decision, is also stored in the personal file of such staff member, and is deleted after a period of 10 years from the end of contract with the concerned staff member.

b) Retention policy for the Informal procedure:

In accordance with the CPVO Retention policy for the working documents used by the Confidential Counsellors during the Informal Procedure implemented in accordance with the CPVO policy on harassment, Confidential Counsellors may not keep any personal data beyond the time needed to deal with a case (data contained in documents such as notes, or electronic communications) and, in any case, personal data cannot be retained for longer than six months following the closure of the Informal procedure.

Where the Informal procedure is closed, and the case is not brought to a Formal procedure, only the opening summary and the closing summary shall be kept, for a period of five years from the date of the closing of the Informal procedure. In these documents, data will be anonymized.

Where the case is brought to a Formal Procedure, data can be kept for a period which shall not exceed five years on the date of the decision to bring the case to a Formal Procedure and will be destroyed after this period. Files may be held for a further five years if there is an administrative or legal procedure (requests from the Ombdusman, CJEU) necessitating their consultation.

During and after the Informal Procedure, for statistical reasons only, a listing of legal precedents within the Office can be created and updated by the Confidential Counsellors. It will ensure total anonymity.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

a) Related to the designation of the Counsellors:

Personal data are stored within Docman on electronic format in a secured Human resources sector file. On paper format, personal data are stored within a locked cupboard of the Human resources sector.

b) Related to the Informal procedure:

The cupboards of the Confidential Counsellors where personal data are stored are locked and duly secured, accessible only to said counsellors. To guarantee the security of confidential data provided in the written exchanges/transmission of documents between the Confidential Counsellors and the Coordinator, these must be delivered by hand in a sealed envelope marked "staff matters" and "private and confidential".

Confidential Counsellors make use of an ad hoc e-mail address specific to the informal procedure, that is, distinct from the professional e-mail address of said counsellors as staff members of the Office. The cited ad hoc e-mail address is password-secured and the privacy of the e-mail communications are duly secured as well.

The Confidential Counsellors and staff members of the Human Resources sector act under the duty of confidentiality.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Legal Advice and Legal Proceedings

2. * Last update of this record:

09/03/2021

3. Reference Number:

No 56

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal service

7. Description of the processing operation:

The Legal service of the CPVO may be requested by other Units and/or services of the Office as well as by external stakeholders to provide legal advice on various issues dealt with by the Office, including the application of the relevant Regulations, contracts, policies, interinstitutional and/or regulatory matters, conflict of interests, internal control related matters, financial and budgetary issues, international relations and cooperation, public access to documents, disciplinary procedures, duties and rights of staff members.

Furthermore, for the purpose of handling legal proceedings such as objections, nullities, cancellations, restitution, revocations, recordals in the CPVR Registers, appeals and actions before the Court of Justice of the European Union, the staff of the Legal service, including the Head of the Legal service, the Legal Advisors, and the Legal Trainees may process personal data when dealing with files kept by the Office.

Additionally, external legal counsels may be appointed to represent the CPVO before the Board of Appeals and/or national courts and/or the CJEU.

8. * Purpose(s) of the processing and legal basis:

The processing of personal data is necessary to enable the provision of the requested legal advice or manage legal proceedings and take decisions.

Legal instruments:

- Internal procedure of 17 November 2011 to be followed by the Legal Officer when drafting legal advice containing personal data.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority);

- Article 5.1(b) of Regulation 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject);

- Article 5.1(c) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract).

9. * Description of the category(ies) of data subject(s):

- Officials, Temporary and Contract Agents;
- Seconded national experts (SNE), Interim Agents and Trainees;
- Parties to proceedings;
- External stakeholders;
- Appointed external Counsels.

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section. The Privacy statement is also published on the CPVO website.

11. * Description of the data or categories of data:

Personal data are processed by the Legal Advisors or external legal counsels, including:

- Name and Surname, e-mail address, postal address, nationality, telephone number of the data subject concerned;
- Statutory link (statutory staff/ or SNE/ or trainees) and if it concerns new recruited staff or not;
- Legal area and a brief outline of the consultation/legal proceedings;
- Type of consultation (by interview / by email / by telephone) and language used;
- No of the file consulted;
- Evaluations of the staff member, grade, rank, indicators of performance;
- Reports issued by disciplinary committee or investigation panel which may contain themselves personal data such as statements, comments and opinions of the staff member.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No. 2018/1725 by submitting a written request to the CPVO data controller, the Head of Legal Service, at dpc@cpvo.europa.eu by *explicitly* specifying the object of the request.

In accordance with the "Administrative Council decision on Internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the CPVO", certain data subject's rights may be restricted, depending on the specific procedure and on a case by case basis.

13. Storage media of data:

Physical copies of documents containing personal data are stored in locked cupboards within the premises of the Office. Electronic copies of the documents are stored in the internal intranet of the Office, Sharepoint, and in the internal database Docman.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data are disclosed to the following recipients on a *need-to-know* basis:

- The President of the CPVO;
- The concerned CPVO staff member;
- The hierarquical superior of the concerned staff member;
- The Human Resources sector.

15. * Period of retention for the data:

The retention period may vary in relation to the specific procedure for which the advice is requested.

If the document is rendered anonymous for historic listing, the Legal Advisor keeps it for an indefinite period. However, if the document still contains personal data which may directly or indirectly identify a staff member the legal advice may be stored by the Legal Advisor during a period of 24 months starting from the date the Legal Advisor transmits the report to the adequate recipients.

Once the legal advice has been provided, physical copies of working documents are promptly deleted.

In case of administrative or disciplinary procedure would arise, please refer to Record No 58 Administrative Inquiry.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to any third country or international organization.

17. * Measures to ensure security of processing :

As regards electronic storage of documents held by the Legal service, both Sharepoint and Docman can be accessed only by CPVO/users within the Offices through the internal network or through the remote VPN SSL. The latter provides access via Two-Factor Authentication (2FA) and databases are username and password protected. In addition, appropriate levels of access are granted individually to the recipients.

As regards physical copies of the legal advice held by the Legal advisor, they are stored within his/her locked cupboard within the Office. Electronic copies stored on the professional device are username and password protected through Windows access.

All the data recipients are bound by statutory and/contractual obligation to observe confidentialy.

*** For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.**

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Requests for Public Access to Documents of the CPVO

2. * Last update of this record:

16/03/2021

3. Reference Number:

No 57

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of processor:

The Register of public access to documents

7. Description of the processing operation:

Within the framework of the procedure for public access to documents of the CPVO, the Office processes compulsory personal data provided by the person requesting access to documents and needed to process the request. The Office may also process any other personal data submitted by the applicant in the request. In addition, the Office processes any personal data that may appear in the requested documents.

The requests for public access to documents of the CPVO follow two types of procedures, the Initial application (the IA) and the Confirmatory application (the CA).

The IA is defined as the first request an applicant will address to the Office. The CA consists of a petition of the applicant to the President of the Office to reconsider the total or partial refusal to grant access to documents contained in the IA.

With a view to address a request to the CPVO Registrar, the CPVO website provides an online application form which the applicant must fill in. In this form, the data subject must indicate his or her identity, address and contact details. The applicant must also specify which documents he or she is asking to be granted access. The applicant has the possibility to add further comments by means of the dedicated box.

a) If the request for access to documents is an "Initial application":

The Registrar receives the initial access application, acknowledges receipt and includes it in the Register dedicated to IAs received. The Registrar then assesses whether the applicant requests access to an administrative document or to a CPVR file, that is, a Plant Variety right application or a CPVR granted title.

In the first case, an answer will be prepared by the relevant services and addressed to the Head of the Legal Service. In case of a request for access to a green file, the Registrar consults the Technical Unit case holder and the Head of the Technical Unit. A draft answer is provided to the Head of the Legal service. In both cases, an answer is sent by email to the applicant.

b) If the request is a "Confirmatory application":

The Registrar receives the confirmatory access application and includes it in the register dedicated to the CAs received. The Registrar sends the application to the President together with a copy of the IA and its answer.

If the CA concerns a CPVR file, a copy of the CA is also sent to the case holder of the Technical Unit and to the Head of Legal Service. The holder of the right concerned is consulted.

The reply of the President of the CPVO is finally sent to the applicant; a copy of it is kept by the Registrar and recorded in the internal database "Docman".

The Head of the Legal service is informed of the President's decision and provided with a copy of the CA.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing activity is to ensure the appropriate handling of requests for public access to documents under Regulation (EC) No 1049/2001. Such requests may be lodged by any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State. It is a general duty of the Office to comply with Regulation 1049/2001, following Article 33a of Council Regulation (EC) No 2100/94. The personal data are collected to assess and to address the answer and/or the documents to the applicant.

Legal Instruments:

- Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents;
- Articles 33a and 88 of Council Regulation (EC) No 2100/94 on Community plant variety rights introduced by Council Regulation (EC) No 1650/2003;
- Article 84 of Commission Regulation (EC) No 874/2009 establishing implementing rules for the application of Council Regulation (EC) No 2100/94 as regards proceedings before the Community Plant Variety Office;
- Practical arrangements adopted by the Administrative Council of the CPVO on 25 March 2004.
- Amendment adopted by the Administrative Council of the CPVO on 19 September 2019 to decision of the Administrative Council of the Office of 25 March 2004;
- CPVO Internal administrative instructions of 13 January 2005 on the Administrative procedure to be followed in relation to request for access to documents of the CPVO;
- CPVO Decision on retention of personal data which are sent by the applicant for a request of access to documents.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

- Applicants for public access to documents;
- Data subjects which personal data appears in the document accessed (where access is granted).

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects on the CPVO website, on the Data Protection section.

11. * Description of the data or categories of data (including, if applicable, special categories of data:

The application form lists the necessary data to be provided by the person requesting access to documents of the CPVO, in order to proceed to the request for public access to documents. Some of the data are mandatory (marked with a star) and other categories of data can be provided on a discretional basis. These data are collected and processed to contact the applicant and are the following:

- Name and Surname; Title;

- Organisation (not mandatory);

- Contact details (professional e-mail address; postal address; phone number).

Regarding the documents to which access can be granted, this includes the following data: a whole file, application form, technical questionnaire, proposal for a variety denomination, photographs, variety description, assignment, and others (to be specified by the public access requestor). Personal data such as name and surnames of applicant breeders and procedural representative (both if legal or natural persons) can be disclosed. Some other personal data, however, may be blanked out/blackened.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Legal service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The CPVO Register of public access to documents. In addition, the form that is sent by the applicant is automatically sent by email to a recipient list (Register and staff members in the Legal service). The form is also filed in Docman together with the answer. No physical copy is either produced or stored.

14. The recipients or categories of recipients to whom the data might be disclosed:

Regarding the application form for public access and information therein contained:

- The CPVO Registrar and assistants to the Registry who receive and compile the requests;

- "Case holders", Technical Unit staff, legal trainees, other Units or services of the Office depending on the requested document;

- The Legal Advisors;

- The President of the Office, in case of CA.

Regarding the data provided upon the grant of the request for access:

- The applicant for public access.

15. * Period of retention for the data:

In Accordance with the CPVO Decision on the retention of personal data which are sent by the applicant for a request of access to documents, data shall be deleted from the internal Docman database/filing system after a retention period of 24 months. During the request processing, should the personal data contained in the application form be transmitted through different staff members by email, each staff member will delete them from his or her email reception box once the personal data transmitted by the applicant are no longer needed by said staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data are not transferred to any third country or international organisation.

17. * Measures to ensure security of processing:

Access to the internal database Docman is username- and password-secured. Regarding incoming and outgoing traffic of electronic communications, an inbound firewall protects the system.

Personal data such as contact details of applicants for CPVR/CPVR titleholders, appearing on documents to which access is granted further to a public access request, is blanked out/blackened. The Office uses a software called "GIMP" for this blacking out of personal data, which cannot be removed and ensure protection of the same.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the Privacy Statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Administrative Inquiry and Disciplinary Procedure

2. * Last update of this record:

12/04/2021

3. Reference Number:

No 58

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The processing operation concerns the management of administrative inquires and disciplinary procedure against CPVO staff members. The procedure develops as here below described.

Prior to any opening of an administrative inquiry, the Head of the Administration Unit consults the Office Européen de Lutte Antifraude (OLAF) on any ongoing investigation from OLAF on the same alleged facts. According to Article 2(1) of the internal rules on administrative inquiries and disciplinary procedures (hereinafter, "the rules"), an inquiry is opened by the President on his own initiative or at the request of a Head of Unit/Service. The decision to open such inquiry designates the Head of Unit/Service responsible of the inquiry, the composition (Article 3 of decision) of the Investigation Panel (IP) and its scope of inquiry. A member of an IP cannot sit on a Disciplinary Board.

The IP conducts its inquiry independently. According to the Article 4(2) of the rules, the IP has the power to obtain documents, summon any person to provide information and carry out on-the-spot investigations. Article 5 of the rules states the conduct of an administrative inquiry. The IP informs the concerned staff member about the inquiry.

The rules also set out that, "a conclusion referring to a staff member by name may not be drawn at the end of the inquiry unless that staff member has had the opportunity to express an opinion on all the facts, which relate to him or her. The Investigation Report shall record that opinion". The staff member's opinions and the records are produced on physical or electronic documents, or orally with written minutes.

The IP submits an Investigation Report to the President after consulting Internal Auditor. Article 5(3) of the rules specifies that the report shall set out the facts and circumstances in question and establishes if the rules and procedures were respected and responsibility was determined. If no charge is brought against a staff member, the closing decision of the inquiry is sent to the staff member who can request to file a copy of the closing decision in his personal file stored by the Human Resources sector. By default, the closing decision of the inquiry is stored in the disciplinary file.

If a charge is brought against a staff member, the Disciplinary Board (DB) takes on the case. The members of the DB are appointed by the President of the CPVO under Article 8 of the rules. Article 8(1) specifies that the record of the hearing is signed by the staff member. A specific training delivered by the European Commission is received by the members of the DB.

The Office ensures complete transparency and that clear information is disseminated to the staff. Record of interviews (of other personnel) are transmitted to the staff member concerned by the inquiry, should these opinions be relevant to the allegations. The collection of personal data in a form of electronic communication is at all moment under strict compliance with Article 36 of Regulation 2018/1725.

8. * Purpose(s) of the processing and legal basis:

The purpose of processing personal data is to collect information and gather evidence, accurate and validly obtained into a file, in order to enable the Investigation Panel to determine whether there has been a failure by an official, servant or other person working for the Office, to comply with his/her obligations under the Staff Regulations of Officials and the Conditions of Employment of Other Servants (CEOS) and to enable the Disciplinary Board to carry out the disciplinary proceedings and hearings.

Legal Instruments:

- Articles 22 and 86, and Annex IX of the Staff Regulations of Officials;
- Articles 49-50a and 119 of the Conditions of Employment of Other Servants (CEOS);
- CPVO Decision of 10 February 2021 on the implementing rules for the conduct of administrative inquiries and for disciplinary procedures;
- Decision of the Administrative Council of the CPVO of 1 April 2020 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the CPVO.

Legal Basis:

Article 5.1 (a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

If, exceptionally, processing of special categories of data within the meaning of Article 10 of Regulation 2018/1725 were to take place, this would be done under strict compliance with the conditions established in this article.

9. * Description of the category(ies) of data subject(s):

- CPVO staff members under investigation;
- Current and former staff members who are not directly concerned but may participate to the procedure (e.g. witness and whistle-blowers);
- Alleged victims.

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Name and Surname, Title, and Functions of the data subjects;
- The action/inaction of the staff member subject to an administrative inquiry and/or disciplinary procedure by reference to the legal definition stated in the Staff Regulations of Officials;
- The penalty imposed on the person concerned (if any);
- Other personal data or document that may be necessary to determine the existence of suspected offences in the framework of administrative inquiries and disciplinary proceedings, in each particular case under investigation;
- Recording of hearings related to investigations and/or disciplinary procedures, including the witnesses' verbal testimony for the purposes of the minutes and under condition that the destruction of the recording

will take place once it has been transcribed to paper. In the event where the data subject would not wish to be recorded for legitimate reasons, he/she informs the CPVO Data Controller.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

As per Article 25(1)(a-i) of Regulation (EU) 2018/1725, exemptions and restrictions may apply in certain cases. In this regard, the CPVO applies Decision of the Administrative Council of the CPVO of 1 April 2020 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the CPVO.

If a restriction provided for by Article 25(1) is imposed, the data subject must be informed of the principal reasons on which the application of the restriction is based and of his/her right to have recourse to the EDPS. Any decision to defer this information should be taken strictly on a case-by-case basis.

In the case of whistle-blowers, informants or witnesses, any restriction to the right of access of these persons will be in line with Article 25 of Regulation (EU) 2018/1725. The identity of whistle-blowers will be kept confidential in as much as this would not contravene national rules regarding judicial proceedings.

Upon request, data subjects have the right to know the origin of the data except where the controller cannot disclose this information for reasons of professional secrecy.

In accordance with Article 26 of the Staff Regulations of Officials and of Articles 11 and 81 of CEOS, CPVO staff members shall have the right to access all data/documents of their personal file and administrative inquiry file and take copies of all documents relevant to the proceedings, including exonerating evidence. The data subject shall execute this right by submitting a written request to the delegated data controller, Head of Administration Unit, at dpc@cpvo.europa.eu.

Regarding the right of rectification, it can only apply to inaccurate or incomplete factual data processed within the framework of this procedure. The controller provides the DPO with access to the record containing the assessment of the necessity and proportionality of the restriction and document the date of informing the DPO in the record. The controller informs the DPO when the restriction has been lifted.

13. Storage media of data:

During the inquiry procedure, information is stored by the authorized IP and DB in paper format in the locked cupboards at the premises of the Human Resources sector.

Electronic copies of documents containing personal data are stored in the internal database Docman in the Disciplinary file and in the personal file.

14. The recipients or categories of recipients to whom the data might be disclosed:

Access and disclosure of personal data is restricted to those who have a legitimate, authorized purpose for gaining access to the personal data:

- Staff member of the Office appointed by the President to conduct the administrative investigation (the Inquiry Panel Leader and/or the Chairman of Disciplinary Board) and his/her alternate;
- Members of the Inquiry Panel or the Disciplinary Board, their alternates;
- Secretary of the Inquiry Panel or the Disciplinary Board, with respect to the personal information transcribed in the minutes of the IP or DB's meetings;
- Legal services for advice regarding the sanction decision;
- If appropriate, the Internal Auditor to be consulted with the concerning Investigation Report before submitting said Investigation Report to the President;
- The President as regards the Investigation Reports and Conclusive Opinions of the Inquiry Panel and the Disciplinary Board;
- OLAF is the recipient of the disciplinary decision;
- The Human Resources sector as custodian of documents generated in the framework of administrative inquiries and disciplinary proceedings. These documents are to be filed in the corresponding personnel files and administrative inquiry files in accordance with the retention policy applied.
- The Human Resources sector sets up and keeps a register of administrative investigations, which shall be declared to the EDPS.
- IT Administrators have access on a *need-to-know* basis.

15. * Period of retention for the data:

Regarding the pre-inquiry file: CPVO retains data for a maximum of two years after the adoption of the decision that no inquiry will be launched. This maximum retention period could be necessary for audit purposes, access requests from affected individuals (i.e.: from an alleged victim of harassment) and complaints to the Ombudsman.

Regarding the inquiry file, there could be three possibilities:
i) The inquiry is closed without follow-up;
ii) A caution is issued; or
iii) The Appointing Authority of the institution adopts a formal decision that a disciplinary proceeding should be launched.

For cases i) and ii), a maximum of 5 years from closure of the investigation is regarded a necessary retention period, taking into account audit purposes and legal recourse from the affected individuals.
For case iii), CPVO shall transfer the inquiry file to the disciplinary file, as the disciplinary proceeding is launched based on the evidence collected during the administrative inquiry.

Regarding the disciplinary file, CPVO (considered the nature of the sanction, possible legal recourses as well as audit purposes) sets up a maximum 20-years-retention period, after the adoption of the final decision. The affected individual may submit a request for the deletion of their disciplinary file 10 years after the adoption of the final Decision. The Appointing Authority shall assess whether to grant this request in light of the severity of the misconduct and the penalty imposed and the possible repetition of the misconduct during that period of 10 years.

A copy of the decision of the DB is stored in the Personal file as well as the copy of the closing decision of an inquiry. The copy of the decision withdrawing the charge after an AI may be stored in the Personal file of the staff member upon his/her request. According to the decision of the President of the CPVO dated 24 March 2021 on the retention period applicable to documents in Personal file, retention period is set as 10 years from the date of the end of the contract. Should the retention period applicable to the Personal file be terminated, the Disciplinary file of the staff member shall not be kept longer.

A staff member against whom a disciplinary measure other than removal from post has been ordered may, after three years in a case of a written warning or reprimand or after six years in the case of any other penalty, submit a request for the deletion from his personal file of all reference to such measure. The appointing Authority shall decide whether to grant this request (Article 27 of Annex IX to the Staff Regulations of Officials).

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to a third country or international organizations.

17. * Measures to ensure security of processing:

When collecting paper information, IP blanks out irrelevant or excessive information to the inquiry.

If electronic information is necessary and relevant to the inquiry, the IT service is responsible for the technical aspects of its collection on the *need-to-know* basis.

Data are stored on computers protected by personal password. Some folders on the Desktop can be accessible via administrative local shares. These shares can only be accessible using the local domain administrator account. The access is restricted by the use of firewalls and the network security scheme. Docman server is not exposed externally.

Logs are maintained of the safeguard of documents (date at which the documents were saved and the user who saved the document).

The only means to communicate data is through the Disciplinary file. Irrespective of the communication channel used, a paper file is prepared by the Head of Unit or HR. Data is stored in paper files kept in locked cabinet and associated e-files are stored on a server with restricted access. Investigators and HR can encrypt e-mails and use locked hardware devices (USB sticks).

The persons in charge of processing data in the context of administrative inquiries and disciplinary

procedures are requested to sign a declaration of confidentiality. The data are not used for any other purposes nor disclosed to any other recipient.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[1]

1. Name of processing:

Time Accounting

2. * Last update of this record:

21/03/2021

3. Reference Number:

No 59

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processors:

DG HR (European Commission)
DG DIGIT (European Commission)
PayMaster Office (PMO) (European Commission)

7. Description of the processing operation:

The processing operation is necessary for the implementation and use of a time accounting system of hours worked by CPVO staff members, with a view to establish credit/debit balances of time worked.

The processing operation concerning Time Accounting (including Flexitime) takes place under the TIM module of SYSPER, the module relating to Time Management. SYSPER is a software created and managed by the European Commission, of which the CPVO makes use. SYSPER requires the processing of personal data in connection with the personal file of each staff member. As described in Record No 68 SYSPER. SYSPER is divided into several modules, dealing with all elements of a staff personal file (mainly CAR (Career), PER (Personal Data), FAM (Family Data) and TIM (Time Management)).

The Time Accounting system for CPVO staff members is managed in the SYSPER timesheets. The data is stored in SYSPER, using timesheets to be filled in per day and totalised per month. Staff members are asked to introduce their hours worked for every day and validate the timesheet at the end of the month. The Head of Unit, President or Vice President verifies the hours and, if agreed, he/she validates the timesheet for agreement. SYSPER calculates automatically the total of hours worked in a month by the staff member and indicates a positive or negative total according to the difference with the mandatory working hours. The total is automatically carried over to the next working month.

In addition, flexitime allows staff to vary the time at which they start and finish their assigned work. Flexitime also allows eligible staff to recuperate, as a secondary option and under certain conditions,

additional hours worked in the form of full days or half days. Such recuperation is always subject to prior approval by the hierarchical superior and taking into consideration the exigencies of the service.

These data is used to have a global overview of the hours worked in a month and indicates if the person has a credit or debit of working hours for the following month. It also indicates if there are sufficient hours worked in a month to be able to ask for flexitime in the following months.

In addition, in the end of the year the accountancy uses data for including it into the annual account at the end of a financial year in order to calculate a provision for the working hours from N (year) which generate flexitime N+1 (year+1).

8. * Purpose(s) of the processing and legal basis:

Legal Instruments:

- Article 55 of the Staff Regulations of Officials;
- Articles 16 and 91 of the Conditions of Employment of Other Servants (CEOS);
- CPVO Decision of 15 February 2019 on Working Time.

Legal Basis:

- Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Official, Temporary Agent, and Contract Agent).

10. When and how were data subjects informed:

The Privacy Statement has been made available to data subjects in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data:

A part of the data being processed for this operation is pre-existing in SYSPER (please refer to Record No 68 SYSPER):
- Name and Surname;
- PerId and Personal Number (NUP);
- The percentage of occupation of post (full or part-time);
- The days of absence (for any type of absence).

As concerns particularly the time accounting system put in place at the CPVO, data subjects must provide with the number of hours worked for every working day.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, the Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.* The CPVO has put in place an Internal Procedure to be followed by the CPVO Controllers in relation to rights exercised by data subjects in accordance with Regulation 2018/1725 dated 20 March 2021.

13. Storage media of data:

Please refer to Record No 68 SYSPER.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- CPVO staff members;
- Administration Unit (Human Resources sector);

Heads of Units/Signing Authority (line manager). External recipients: DG HR (European Commission); DG DIGIT (European Commission); PayMaster Office (PMO) (European Commission).
15. * Period of retention for the data: The data are kept in SYSPER as long as the staff member is in active service. Please refer to Record No 68 SYSPER.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: The personal data is not intended to be transferred to a third country or international organization.
17. * Measures to ensure security of processing The measures in place to ensure the security of processing are those concerning SYSPER. Please refer to Record No 68 SYSPER.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Access to Applications of the European Commission

2. * Last update of this record:

14/04/2021

3. Reference Number:

No 60

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)
IT Unit (IT System Administrator)

External processor:

SYSPER (European Commission)
PayMaster Office (PMO) (European Commission)
DG DIGIT (European Commission)

7. Description of the processing operation:

CPVO staff members have access to certain services issued by the European Commission, including online applications facilitating exchanges between institutions and further services, as the Joint Sickness Insurance Scheme (JSIS), PMO Contact and e-learning modules.

Staff members may access the services through the European Commission's Authentication System. The Human Resources sector provides name and surname of the staff members to the IT System Administrator to facilitate the access to the services to staff members. The IT System Administrator uploads an Excel sheet with names and surnames of the staff members in the intranet of SYSPER, through the module "Identity Management (COMREF/RETO)". The system automatically synchronizes the data available in the Excel sheet with data in SYSPER, and once this Excel sheet is uploaded, a unique identification number is created (PerID). This process allows the creation of a profile for each staff member in order to gain access to the services though the European Commission's Authentication System.

The system provides the opportunity to use the Two-Factor Authentication (2FA) system, so the IT System Administrator may gather personal or professional phone number of the staff for security purpose. An update is sent monthly by the Human Resources sector to the IT Administrator with relevant changes to be introduced in the intranet of SYSPER.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is providing to CPVO staff members access to the Commission on-line applications and platform facilitating exchanges between staff members and relevant EU offices/bodies through the ECAS portal.

Legal instruments:

- Articles 24(a) and 45(2) of the Staff Regulations of Officials (online trainings);
- Articles 11 and 85(3) of Conditions of Employment of Other Servants (CEOS) (online trainings);
- Annex VII Section 3 to the Staff Regulations of Officials (reimbursement of expenses).

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO Staff members, Seconded National Experts, Trainees.

10. When and how were data subjects informed:

The Privacy Statement is made available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

The Privacy Statement of SYSPER module "Identity Management (COMREF/RETO)" adopted is also available in the intranet of the office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The data collected are:

- Name and surname of the staff member;
- Personnel number of the staff member;
- Date of birth of the staff member;
- Professional e-mail address of the staff member;
- Personal mobile phone number of the staff member.

Additional data may be collected through the identification portal ECAS, including:

- Date and time of last password change or reset, date and time authentication;
- Number of logs;
- Recent passwords;
- IP address.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EC) No. 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The Excel sheet containing the list uploaded in the Intranet of SYSPER is stored in an internal server within the premises of the Office by the IT System Administrator to which only he/she has access.

As regard external processors, data are also stored in the ECAS portal as well as within servers of the external processor.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal Recipients:

- Human Resources;
- IT System Administrator.

External Recipients:

- SYSPER (European Commission);
- PayMaster Office (PMO) (European Commission);
- DG DIGIT (European Commission) for maintenance and authentication purposes.

15. * Period of retention for the data:

As regards the Excel Sheet to be uploaded in the Intranet of SYSPER, the document is updated and uploaded in the Intranet of SYSPER on a monthly basis, and older electronic copies of the updates introduced are manually deleted once the new documents are introduced.

As regards the external service provider, please refer to Record No 68 SYSPER and the Privacy Statement of the module "Identity Management (COMREF/RETO)".

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to any third country or international organization.

17. * Measures to ensure security of processing:

Only the IT System Administrator has access to the internal server where the documents are stored. Access to the server is username- and password-protected.

Access through the ECAS portal is password-protected and CPVO staff members may avail themselves of the Two-Factor (2FA) authentication to access the service.

Regarding the external service provider, please refer to Record No 68 SYSPER and the Privacy Statement of the module "Identity Management (COMREF/RETO)".

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Internet Filtering Policy

2. * Last update of this record:

08/02/2021

3. Reference Number:

No 61

4. * Name and contact details of the Controller:

Head of IT Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

IT Unit

7. Description of the processing operation:

The proxy system is a web security gateway integrated into the ICT infrastructure of the CPVO. It uses filtering techniques by automatically blocking inappropriate websites. In particular, when a user in the office accesses the internet, the request will be processed through a proxy "squid " system in the firewall. With this system, when a user requests access to a page, "squid" will check if the user is authorized against CPVO AD and if the URL asked is not blacklisted (SquidGuard, University of Toulouse lists). It will then serve the page to the user and log the categories of data mentioned in point 11.

The IT System Administrator may only access and render identifiable these logs in the event of a disciplinary procedure, suspected breach of the Staff Regulations, investigations or judicial inquiries from legal authorities, with approval by the President of the Office and in the presence of the DPO.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing of the proxy "squid" system is to provide additional security and a mechanism for enforcing the ICT User policy of the CPVO ensuring thus the functionality of the network and avoiding security breaches.

Legal instruments:

- CPVO Policy of 1 January 2020 on the Use and Monitoring of CPVO Communications and IT tools.

Legal Basis:

Article 5(1)(a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

The data subjects include everyone who uses Internet services at the CPVO. This includes CPVO'S staff and trainees, as well as employees of service providers or any other person making use of the CPVO's information and technology infrastructure.

10. When and how were data subjects informed:

The Privacy Statement and the CPVO Policy on the use and monitoring of CPVO communications and IT tools are made available to staff on the intranet of the Office, Sharepoint.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- User identification (username);
- Date and time of the access to the Internet;
- Browsing time (timestamp);
- Client IP (internal IP of the computer requesting the web page);
- Results of codes;
- Size (the amount of data delivered to the client);
- Request method to obtain an object;
- Relative URL visited;
- Transaction duration;
- IP address or hostname of the forwarded request;
- Content type of the object seen in HTTP reply header.

All these data are recorded automatically by the system as log files.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 submitting a written request to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu by *explicitly* specifying *the request.*

13. Storage media of data:

All log files are stored on a server, protected by a complex password and only accessible by the IT System Administrator. The server is located within the CPVO premises.

14. The recipients or categories of recipients to whom the data might be disclosed:

The IT System Administrator may only access and render identifiable these logs in the event of a disciplinary procedure, suspected breach of the staff regulations, investigations or judicial inquiries from legal authorities, with approval by the President of the Office and in the presence of the DPO.

The CPVO does not monitor the use of CPVO Communication Tools unless there are legitimate reasons for doing so. Examples of legitimate reasons would be an investigation due to suspicion of breach of CPVO rules and policies, the Staff Regulations or criminal legislation.

15. * Period of retention for the data:

The logs are kept for 6 months, period after which they are manually deleted.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if shuch is the case:

The personal data is not intended to be transferred to any third country or international organizations.

17. * Measures to ensure security of processing:

All log files are stored on the server which is protected by a complex password only accessible by the IT System Administrators. The server is located in a locked server room which access is restricted to authorized staff only.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

---

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Prevention and Management of Conflicts of Interest

2. * Last update of this record:

25/03/2021

3. Reference Number:

No 62

4. * Name and contact details of the Controller:

Head of Legal service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal Service

7. Description of the processing operation:

The CPVO Procedure for the Prevention and Management of Potential Conflicts of Interest foresees that individuals working for or with the Office shall declare any interests which could be considered to be prejudicial to their independence. Model declarations to be signed by data subjects can be found as Annexes in the CPVO Procedure for the Prevention and Management of Potential Conflicts of Interest.

A conflict of interest refers to a situation where the impartiality and objectivity of a decision, opinion or recommendation of an Agency is or might be perceived as being compromised by a personal interest held or entrusted in a given individual.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing activity is to prevent and manage issues of conflict of interest in the CPVO, to ensure transparency, integrity and accountability, and to enforce the European Commission Guidelines on the prevention and management of conflicts of interest in EU decentralized agencies of 10 December 2013.

Legal Instruments:

All data subjects:

- European Commission Guidelines on the prevention and management of conflicts of interest in EU decentralised agencies of 10 December 2013;

- CPVO Policy on prevention and management of conflict of interest adopted by the CPVO Administrative Council of March 2018.

CPVO Administrative Council:

- Article 33 and 39 of Regulation (EU, Euratom) 2018/1046 on the financial rules applicable to the general budget of the Union (adoption of the budget);

- Articles 36, 109, 111 and 112 of Council Regulation (EC) No 2100/94.

CPVO Management (President, Vice-President, and Heads of Units):

- Article 61 of Regulation (EU, Euratom) 2018/1046 on the financial rules applicable to the general budget of the Union;

- Article 42 of Council Regulation (EC) No 2100/94;

- Articles 39 and 42 of the CPVO Financial Regulation (DOC-AC-2015-2-6-Annex 1-EN);

- Article 2 of the Code of good administrative behaviour of the European Commission of 20 October 2000.

CPVO staff members:

- Articles 11, 11(a)(1), 12(b)(1), 13, 16, 17(1), 17(2), 19, and 40 of the Staff Regulations of Officials;
- Articles 11, 17, 52 and 81 of the Conditions of Employment of Other Servants (CEOS);
- Article 42 of the Financial Regulation of the CPVO (DOC-AC-2015-2-6-Annex 1-EN);
- Article 2 of the Code of good administrative behaviour of the European Commission of 20 October 2000.

CPVO Committees:

- Code of good administrative behaviour of the European Commission of 20 October 2000.

Members of the CPVO Board of Appeal:

- Article 47 and 48 of the Council Regulation (EC) No 2100/94.

Seconded National Experts:

- Decision on seconded national experts (DOC-AC-2018-1-13);

- Code of good administrative behaviour of the European Commission of 20 October 2000.

Examination Offices:

- Articles 55 and 56 of Regulation (EC) 2100/94;
- Article 15(1) of Regulation (EC) 874/2009;
- Entrustment Requirements for CPVO Examination Offices (DOC-AC-2015-2-21-EN).

Audit Advisory Board and Audit Experts:

- Articles 78, 79 and 80 of the Financial Regulation of the CPVO (DOC-AC-2015-2-6-Annex 1-EN).

Calls for tenders and contractors:

- Article 42 of the Financial Regulation of the CPVO (DOC-AC-2015-2-6-Annex 1-EN).

Legal basis:

Article 5(1)(a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Members of the CPVO Administrative Council, members of the CPVO Management Team, CPVO staff members, members of the CPVO decision Committees, members of the CPVO Selection Committee, members of the CPVO Board of Appeal, seconded national experts, members of the Audit Advisory Board, data subjects representing the Examination Offices, other external contractors (e.g.: within the framework of call for tenders).

10. When and how were data subjects informed:

The data subjects, at the time of beginning their duties vis-à-vis the Office, are informed about the CPVO Policy on Prevention and Management of conflict of interests and sign a declaration to this effect.
A Privacy Statement is made available to data subjects in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following categories of data are processed:

Declaration of interests for members of the Administrative Council:

- Name and Surname;
- Title;
- Previous and current activities;
- Details of any posts and/or professional activities carried out over the previous two years which may potentially impact as to impair the person's independence in their activity as AC member or alternate member;
- Posts currently held or activities currently being carried out which may have a potential impact such as to impair the person's independence in their activity as AC member or alternate member;
- Shares and/or stocks beyond the relevant threshold in the capital of companies having an interest in or related to the field of activity of the CPVO, which may have a potential impact such as to impair your independence in your activity as AC member or alternate;
- Ownership or other investments, including shares, in breeding companies, exceeding the relevant minority control threshold (period, name/location of the organization, subject matter);
- Information concerning membership of a managing body or equivalent structure in a breeding company/plant related research centre (period, name/location of the organization, subject matter);
- Information concerning membership of a scientific Advisory Body, of an agricultural/horticultural research institute (period, name/location of the organization, subject matter);
- Information regarding Consultancy or advocacy for an environment/food/IP- related NGO (period, name/location of the organization, subject matter);
- Employment (period, name/location of the organization, subject matter);
- Information concerning research funding, for example fund received from private companies for research activities in this domain (period, name/location of the organization, subject matter);
- Ownership of Intellectual property information (period, name/location of the organization, subject matter);
- Other membership or affiliation (period, name/location of the organization, subject matter);
- Interests of close family members i.e.;meaning spouse, partner, children and direct ascendants (period, name/location of the organization, subject matter);
- Signature.

Declaration of interest for members of the Management Team or of members of CPVO Committees:

- Name and title;
- Nature and range of activities;
- Ownership or other investments, including shares, in breeding companies, exceeding the relevant minority control threshold (period, name/location of the organization, subject matter);
- Information concerning membership of a managing body or equivalent structure in a breeding company/plant related research centre (period, name/location of the organization, subject matter);
- Information concerning membership of a scientific Advisory Body, of an agricultural/horticultural research institute (period, name/location of the organization, subject matter);
- Information regarding Consultancy or advocacy for an environment/food/IP-related NGO (period, name/location of the organization, subject matter);
- Information regarding the involvement in research funding, for example, fund received from private companies for research activities in this domain (period, name/location of the organization, subject matter);
- Intellectual property information (period, name/location of the organization, subject matter);
- Other membership or affiliation (period, name/location of the organization, subject matter);
- Interests of close family members i.e. meaning spouse, partner, children and direct ascendants (period, name/location of the organization, subject matter).

Declaration of absence of conflict of interests and of confidentiality in calls for tenders:

- Name and signature.

Declaration of independence and confidentiality for Seconded national experts:

- Name and signature.

Declaration of integrity for CPVO staff members:

- Name and signature.

Declaration of honour for CPVO staff members leaving the CPVO services:

- Name, address, pension number, telephone, and signature.

Declaration of intention to engage in an occupational activity after leaving the CPVO:

Staff members sign a declaration of integrity form upon appointment and both a declaration on honour and an occupational declaration, when necessary, upon termination of contract. These form and declarations concern the processing of the following categories of data:
- Name and Surname;
- Title;
- Personnel number;
- Function group/grad/step;
- Address;
- Telephone and fax number;
- E-mail address;
- Whether the person is receiving or will receive any pecuniary benefit from the CPVO after leaving. If so, of what sort;
- New activity: name of the body, address, telephone and fax number, e-mail address, nature of the new activity, whether the body receives funding from the European Commission or the CPVO, description of the new activity, expected duration, expected starting date, whether the person will be an employee, shareholder or self-employed;
- Whether the person will receive a remuneration or other pecuniary advantages and to specify if so, whether the body has a direct or indirect commercial, financial or contractual links with an EU Institution or body and, if so, whether the person had direct or indirect relations with the body for which he/she wishes to work during his/her work at the CPVO.
- Whether the new activity will have direct or indirect links with the former service, other CPVO services and to specify;
- Signature.

Declaration of independence for CPVO Board of Appeal members:

- Name and signature.

Annex to the Designation Agreement of entrusted Examination Offices:

- Signature;
- No other personal information involved except if conflict of interest is linked to identified individuals, case in which the following data are required: Name and position in Examination office, information on conflict of interest.

Declaration of integrity for Audit experts:

- Name and signature.

Declaration of confidentiality- Audit Advisory Board:

- Name and signature.

Declaration of independence for Selection Board members:

- Name and signature.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No. 2018/1725 by submitting a written request to the CPVO data controller, Head of Legal Service, to dpc@cpvo.europa.eu.

13. Storage media of data:

Electronic copies of personal files are stored in the internal database Docman, and physical copies of personal files are stored in a cupboard at the premises of the Human Resources sector.

14. The recipients or categories of recipients to whom the data might be disclosed:

Authorised CPVO staff members (Reporting Officer, Appointing Authority, Human Resources Sector, Legal Service), as well as IT Administrators on a *need-to-know* basis. The Declaration of Interest of the members of the Administrative Council and Board of Appeal could be made publicly available on the CPVO website.

15. * Period of retention for the data:

In each case, the period of retention of the personal data corresponds to the duration of the mandate of the function to which the declaration refers, or to the period of validity of the declaration if such is indicated.

In what concerns financial personal data and documents in support thereof, and in accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, these are kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

As for personal data in the files of CPVO staff members, and in accordance with CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, these will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not transferred to a third country or international organization.

17. * Measures to ensure security of processing:

Access to the internal database Docman is username- and password-secured and can be accessed by the official in Human Resources sector. The physical files containing the data are locked in cupboards in the Human Resources premises.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Quality Audit Services (QAS) Activities

2. * Last update of this record:

03/04/2021

3. Reference Number:

No 63

4. * Name and contact details of the Controller:

QAS Team Leader
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Quality Audit Service (QAS)

External processors:

Microsoft
Microsoft sub-processors
Afixed employee from Uplink

7. Description of the processing operation:

The CPVO operates an accreditation scheme for Member State – Examination Offices, including their Technically Qualified Bodies and their subcontractors, if any, performing DUS testing on varieties for which a CPVR application has been filed. The evaluation of the Examination Offices' competences are carried out by a regular assessment (every 3 years) through the QAS. The QAS performs an independent function to ensure and establish competence of the examination of EOs and reports directly to the Administrative Council. The QAS' function requires to assess the competence of the entire operations of Examination Offices, as well as the Technically Qualified Bodies and their subcontractors if any, including the competence of the personnel. In order to to carry out this latter assessment, contact information and personal information contained in documents demonstrating the competence required of the persons involved in DUS testing are processed. Moreover, in doing such work the QAS Team Leader is assisted by technical experts that are chosen among a List of Technical Experts in entrustment assessments approved by the Administrative Council. Said experts are assigned on a needs basis for individual on-site visits. Finally, it has been envisaged the possibility to have a substitute QAS Team Leader in case of temporary incapacity of the current QAS Team Leader. In this respect, a list of six substitute QAS Team Leaders that have been formally appointed by the Administrative Council.

The QAS at CPVO, collects and retains personal information such as name, surname, email and other details set out in the CV (like birthday and age) of the staff of Examination Offices, Techinically Qualified

Bodies and their subcontractors if any, as well as technical experts participating in the audit and substituting QAS Team Leader. Photos may be taken for communication purposes.

Due to the outbreak of the coronavirus COVID-19 pandemic, the Office has extended the use of 'Microsoft Teams' ('MS Teams'), as part of Microsoft Office 365, to organise virtual meetings and videoconferences remotely with internal staff and external stakeholders, including for the QAS Service activities.

MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services. Virtual meeting/sessions might be recorded with the aim of making available further material to the data subjects. In case of recording, participants to QAS actvities on MS Teams are duly informed and required to give their consent in advance.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is to establish the competence of examination offices through interviews of official staff and to provide a sound basis for entrustment decisions of the Administrative Council as well as to recruit the technical experts that should assist the QAS team leader as well as those who might substitute the Team Leader in case of temporary incapacity.

Pictures of the assessment exercises, including the participants on said assessment, may be taken for communication purposes. For more information, please refer to Record No 12 Social Media.

Legal Instruments:

- Articles 30(4), 55, 56 and 57 of the Council Regulation (EC) No 2100/94;
- Contractual arrangement between Examination Offices and the CPVO (Designation agreement);
- Entrustment Requirements approved by Administrative Counicl, of 15 October 2015;
- CPVO Technical protocols for DUS testing;

Legal Bases:

- Articles 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);

- As regards the taking of photos and recording of virtual meetings, Article 5.1 (d) of Regulation (EU) 2018/1725 (the data subject has given consent to the processing of his or her personal data for one or more specific purposes).

9. * Description of the category(ies) of data subject(s):

- Employees of the EOs involved in technical examinations;
- Employees/ Staff of TQBs performing technical examinations on behalf of the EOs entrusted;
- Subcontractors of TQBs involved in technical examinations;
- QAS technical experts;
- Substitute QAS Team Leaders.

10. When and how were data subjects informed:

The Privacy Statement is sent to every examination office by e-mail before each assessment as part of the audit announcement.

The Privacy Statement is also sent to the QAS technical experts and substitute QAS Team Leaders upon their appointment.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Names and surnames;
- Email;
- Postal address;
- Date of birth (or age);

- Responsibility in DUS work;
- Personal training records;
- Curriculum Vitae;

Photos of participants in assessment exercises may be taken for communication purposes.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EC) No. 2018/1725 by submitting a written request to the CPVO data controller, QAS Leader, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The documents and associated files containing personal data are kept in the document management system of CPVO , with defined access authorisations limited to the QAS leader and, when necessary, to the appointed substitute QAS Team Leader.

As for Microsoft, data are stored in Europe. However, additional data may be available to sub-processors outside the EU. Personal data are collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data are disclosed to QAS Team Leader and, when necessary to the appointed substitute QAS Team Leader. Access to specific information to other parties is limited to situations where this is needed in order to fulfil a function defined in one of the regulations governing the operations of the CPVO. In particular,
- QAs External experts involved in QAS' activities, on a need to know basis.
- Audit Advisory Board (AAB), on a need to know basis. Data might be disclosed when objections on the final assessment report are raised by the EO. This might happens also in case of complaints involving the QAS as well as when providing advice in the continuous development of the system.

In exceptional circumstances, personal information of QAS' Technical Experts might be transferred to the Ministry of Agriculture and Rural Affairs, P.R. China (MOARA), with the aim of strengthening the cooperation between EU and China, in light of the IP Key China Project, of which the CPVO is partner.

15. * Period of retention for the data:

Hard copies of documents containing personal data will be retained for six years in accordance with Article 8.3 of the QAS entrustment procedure manual. Electronic files are kept for an undetermined period. The CVs of QAS technical experts involved in QAS are retained for eight years.

As regards data processed under MS Teams, the data is retained for one year after the exchange activity is completed.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

In exceptional circumstances, personal information of QAS' Technical Experts might be transferred to the Ministry of Agriculutre and Rural Affairs, P.R. China (MOARA), with the aim of strengthening the cooperation between EU and China, in light of the IP Key China project, of which the CPVO is partner.

As regards the use of MS Teams, most customer data are kept in Europe, but additional data might be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

17. * Measures to ensure security of processing:

The CPVO:

Assessment records and associated files are kept in the document management system, according to the security standards, with defined access authorisations. The information is stored securely so as to

safeguard the confidentiality and privacy of the data therein. Dissemination of personal records such as CV's of EO personnel is restricted and particularly accesible only to the QAS Team Leader or, when necessary, to the appointed substitute QAS Team Leader.

Microsoft:

Microsoft implements appropriate technical and organisational measures to safeguard and protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them. Office 365 has been configured to preserve the confidentiality of the information exchanged by implementing encryption during all communications and in storage, and anonymous access is not authorized. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. Datacentres have physical and logical security monitoring measures. Finally, Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Whistleblowing Procedure

2. * Last update of this record:

31/03/2021

3. Reference Number:

No 64

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

Whistleblowing procedures are intended to provide safe channels for anyone who becomes aware of and reports potential fraud, corruption, or other serious wrongdoing and irregularities. Whistleblowing procedures protect whistleblowers and disclosures that are in the public interest.

In accordance with Article 22(a) of the Staff Regulations of Officials, CPVO staff members are obliged to report suspicions of serious irregularities affecting the Office. Such reports should be made in writing and may be made either internally within the CPVO or externally to OLAF.

As regards Internal Whistleblowing, there are two options:
- Staff members who, in the course of or in connection with their duties, discover that serious irregularities may have occurred or may be occurring, are obliged to report this discovery forthwith and in writing to either their immediate superior or to their President or Head of Unit/Service.
- If there is a concern that this disclosure may lead to retaliation or that the intended recipient of the report is personally implicated in the serious irregularities, then the staff member may also bypass this direct means of internal reporting and address his or her report directly to OLAF. OLAF may also be notified through the Fraud Notification System. In any case, the recipient of the information is in turn obliged to transmit the information thus received without delay to OLAF. Once reports are submitted to OLAF, OLAF's relevant policies apply.

As regards External Whistleblowing (option of last resort), upon receipt of the information reported internally, OLAF or the CPVO must give the whistleblower within 60 days of receipt of the information an indication of the period of time considered reasonable and necessary to take appropriate action. If no action is taken within that period of time, or if the whistleblower can demonstrate that the period of time set is unreasonable in light of all the circumstances of the case, he or she may make use of the possibility of external whistleblowing as provided for in Article 22(b) of the Staff Regulations. If neither the CPVO nor OLAF has taken appropriate action within a reasonable period, the staff member who reported the wrongdoing has the right to bring his or her concerns to the attention of the President of either the

Council, the Parliament or the Court of Auditors, or to the Ombudsman. In this case, the whistleblower protection continues to apply.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing operation is to enable the reporting of fraud, corruption or other serious professional wrongdoing in the CPVO, to establish reporting channels for whistleblowers, to manage and follow-up reports, and to ensure protection and adequate remedies for whistleblowers.

Legal instruments:

- Articles 11, 21(a), 22(a), 22(b) and 22(c) of the Staff Regulations;
- Articles 11 and 81 of Conditions of Employment of Other Servants (CEOS);
- Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, 2018/0106;
- CPVO Guidelines on Whistleblowing of 15 February 2019 (DOC-AC-WP-2019-1-Annex III c);
- Decision of The Administrative Council of the CPVO of 30 September 2020 on Administrative Inquiries and Disciplinary Procedures (DOC-AC-2020-2-15-Annex 2) (Adoption by Analogy of Commission Decision C(2019) 4231 of 12 June 2019 on Administrative Inquiries and Disciplinary Procedures);
- EDPS Guidelines on processing personal information within a whistleblowing procedure of December 2019;
- Practical Guide to Staff Ethics and Conduct, Section on Reporting serious wrongdoing (Whistleblowing).

Legal basis:

Article 5.1 (a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO staff members (Officials, Temporary Agents, Contract Agents), Seconded National Experts, trainees and interim staff.

10. When and how the data subjects were informed:

Information to data subjects is provided in CPVO Guidelines on Whistleblowing, as well as in the Privacy Statement available on the CPVO's Intranet, Sharepoint. Trainings specifically devoted to Whistleblowing Procedures are also provided to the CPVO staff members.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The personal data are contained in the report submitted by the whistleblower and any subsequent document drawn up in response to that initial report. These documents may contain names, contact details, and other personal data. In principle, special categories of data should not be included.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subjects rights are foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725. A written request should be submitted to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

Data subject rights could be restricted in accordance with the CPVO Administrative Council Decision on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the CPVO [CPVO Internal Rules concerning Article 25 of Regulation (EU) No 2018/1725].

13. Storage media of data:

Irrespective of the communication channel used by the whistleblower, a file is prepared by the Head of Unit or the Human Resources sector, depending on whom the report is addressed to. This data is stored in paper files kept in locked cupboards. Electronic files are stored on a server with restricted access.

14. The recipients or categories of recipients to whom the data might be disclosed:

Access is granted to internal and external recipients on a strict *need-to-know* basis.

Internal recipients:

- The immediate superior of the staff member concerned;
- The Head of Unit/Service concerned;
- The President;
- The Human Resources sector.

External recipients:

-OLAF
-Ethics Correspondents (if contacted by the Whistleblower).

15. * Period of retention for the data:

Different retention periods are applied depending on the information reported and how the case is dealt with. If following an initial assessment it is clear that the case should not be referred to OLAF or is not within the scope of the whistleblowing procedure, the report is deleted as soon as possible.

In any case, personal data are deleted promptly and in any case within two months from the date on which the whistleblower reported the alleged incident and the file is finally closed without follow up. Longer retention periods may be envisaged on account of specific circumstances requiring so. For instance, depending on the nature of the information.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

The organisational structure includes defined responsibilities for the various aspects of data protection at several stages of the whistleblowing procedure.

All CPVO staff members are bound by an obligation of confidentiality. Only the whistleblower who reports the wrong-doing may give access to the data to a (line) manager, who is responsible to keep confidential the information and report it to the appropriate level. Sharing of confidential information documents or extending the access rights requires a decision by someone with appropriate authority.

A safe for storage of particularly sensitive physical documents has been acquired by the CPVO. Only relevant CPVO staff members have access to the files for the purpose of investigating the whistleblowing report (namely, the person to whom the wrongdoing was reported, hierarchical superiors and HR officer) and are instructed not to keep copies after completion of the whistleblowing procedure.

The paper files are stored in locked filing cupboards by the officers handling the whistleblowing files. The electronic files are stored on servers with restricted access limited to staff member(s) identified on a *need-to-know* basis. The access is restricted by the use of firewalls and the network security scheme (including a DMZ). Human Resources staff members can also encrypt e-mails and use locked hardware devices (USB sticks).

The only means to communicate data is through whistleblowing reports. Irrespective of the communication channel used by the whistleblower, a paper file is prepared by the Head of Unit or HR Service, depending on whom the reports is addressed to.

In cases where the information provided by a whistleblower contains personal data that are clearly not needed for examining the issues raised in the report, these data will be erased from the report, if necessary after consulting the whistleblower, to the extent that this is possible without resulting in the substantive examination being unduly delayed.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

---

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Access Card System

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 65

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

IT Unit

7. Description of the processing operation:

The access cards system's key pad and sensor are placed at each external door, in particular:

The main building "HBM":
- Main Entrance;
- Side Entrance;
- Garage;
- Archives Registry;
- Archives Accounting and Finance sector;
- Archives Technical Unit;
- Parking plots.

"Mirror" building:
- 2nd Floor entrance;
- Ground floor entrance.

Technical Unit building:
- Main Gate;
- Main entrance;
- Side entrance;
- Garage bicycles.

Each CPVO staff member, external contractor and trainee is given an access card, which allows to access CPVO premises, as mentioned above. Access cards' ID is linked to a particular person. Each time the data subject uses an access card, the log is kept, which comprises access date and time by particular access card and door location.

8. * Purpose(s) of the processing and legal basis:

The purpose of using the access cards is to ensure the safety and security of CPVO buildings, assets, staff and visitors. The access card 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.

Personal data (logs) are accessed only when necessary for ensuring the security and safety of premises, individuals and goods particularly, in case of investigating a security incident. The data are not used for any other purpose other than that described above.

Legal instruments:

- Article 30 of the Council Regulation (EC) No 2100/94 on Community plant variety rights;
- CPVO procedure of 2 July 2019 on Security Guards.

Legal basis:

Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

CPVO staff members, authorised external contractors, trainees.

10. When and how were data subjects informed:

The Privacy Statement is made available in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- Name and Surname;
- Access card ID, which is linked to particular person;
- Access time, date and door location.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of IT Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

The data are kept digitally on the hard drive of the server.

14. The recipients or categories of recipients to whom the data might be disclosed:

The logs may be monitored only in case of a security incident or as a result of the access request from the data subject. The log is viewed by the Controller who is responsible for investigating the security incidents and granting access right to the logs. Logs are accessed by IT System Administrator only on President request, for example in case of official inquiry.

15. * Period of retention for the data:

Personal data contained in the logs generated by the access card are kept for 30 days and then destroyed.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing: The system's hard drive is stored in securely locked room. Access server is highly limited, being protected by a password and recording any log or action from the staff members. Data can only be accessed by the IT System Administrator following the authorization of the President.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Online Trainings

2. * Last update of this record:

23/03/2021

3. Reference Number:

No 66

4. * Name and contact details of the Controller:

Head of the Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processors:

Administration Unit (Human Resources sector, Finance and Accounting sector)
IT Unit

External processors:

- Altissia
- EU Learn Portal
- LinkedIn

7. Description of the processing operation:

The processing operation consists in the offering to CPVO staff members of online trainings that help them in acquiring or developing new knowledge or skills in key areas for their performance of their tasks.

There are two types of courses in which CPVO staff members may participate: those for which a license/account has been granted to staff, and those for which no such license/account has been granted. The main external training platforms of which the CPVO makes use are Altissia, EU Learn Portal and LinkedIn.

- Courses for which a licence/account has been granted to staff:

Online training courses in a variety of subjects can be attended by staff members, by benefiting from one of the licenses/ accounts acquired or created by the Office, upon request or by indication from their corresponding Head of Unit. In some cases, staff can attend trainings on their own initiative. Licence/ account attribution is handled by the Head of Administration and by the Human Resources sector.

The CPVO Head of Administration or staff members of the Human Resources sector manage the licenses/accounts allocated to staff for the use of online training. The personal information included to allocate the license is the name and surname of the staff members as well as his/her professional e-mail (not in all cases all these data is needed and in some cases is enough with the email address).

The Head of Administration has the possibility to create playlists of voluntary training for staff to be used as indicative useful training courses.

Moreover, the Head of Unit can also compile a list of compulsory training that will be communicated to the Human Resources sector and notified to the staff members. Staff members will be required to complete the trainings in a certain period of time in order to enhance their knowledge and performance of their tasks in the required areas considered by the Head of Unit. The Human Resources sector is then notified of the completion of the compulsory course.

- Courses for which no licence/account has been granted to staff:

A staff member wishing to follow a training course agreed with his/her reporting officer either within his/her CDR ("Development Plan for the year") or on an ad-hoc basis has to apply for a course using the CPVO internal IT platform to request training ("Centurio"). Applications shall be approved by the relevant Head of Unit. Applications should be filled with at least one month of anticipation before the period foreseen for the training or before the final enrolment date.

Once the application is approved by the relevant Head of the Unit, the personal data, in particular the name, surname, email, could be passed to the external training company, responsible for providing the certain training, in order to contact the staff member concerning the training and issue a certificate of the attendance in the end of course.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is offering to CPVO staff members online training support, with a view to enhance the knowledge or skills of staff members in key areas for the performance of their tasks.

In order to attribute license/account that are not used by participants, the level of utilisation is monitored. Resource allocation and statistics are the main reasons for this monitoring, under no circumstances the data will be used for evaluation of an individual's performance, except if the training was done on request of the line manager.

Legal instruments:

- Articles 24(a) and 45(2) of the Staff Regulations of Officials;
- Articles 11 and 85(3) of CEOS;
- CPVO training policy of 26 June 2014.

Legal basis:

- Article 5.1 (a) of Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members, Seconded National Experts and Bluebook Trainees.

10. When and how were data subjects informed:

The Privacy Statement has been made available for data subjects in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The categories of data being processed are the following:
- Name and Surname;
- Administrative status, Grade and CPVO Unit and service;
- Personal number;
- Mother tongue and other languages;
- E-mail address of participants.

Note: an exception has been implemented for the access to LinkedIn Learning portal. An anonymised e-mail address (alias) is used for the training purpose (granting of a license) to avoid the identification and link with the main LinkedIn account (professional network).

The online training providers may also have access to the following data:
- IP Address;
- Date and time of access to the site;
- Pages browsed;
- Type of browser used;
- The platform and/or operating system installed on the device (computer, tablet, smartphone);
- The search engine and keywords used to find the site.

Additional data may optionally be provided by participants when, for example, taking part in discussions or posting contributions through the website. These data are not required to participate in the courses and are provided by and at the discretion of the data subject.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The Data Subjects rights are foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725. The data subject can submit a request to the CPVO data controller, Head of Administration Unit by explicitly specifying the request at dpc@cpvo.europa.eu. The CPVO has put in place an Internal Procedure to be followed by the CPVO Controllers in relation to Rights exercised by data subjects in accordance with Regulation 2018/1725 dated 20 March 2021.

The data subject can also submit a request to the online training providers to exercise his/her rights. In this case, please refer to the respective privacy statements of Altissia, EU Learn, and LinkedIn:
- Altissia: https://altissia.org/privacy-policy/
- EU Learn: https://europa.eu/learning-corner/learning-corner-privacy-statement_en
- LinkedIn: https://www.linkedin.com/legal/l/dpa

13. Storage media of data:

Electronic copies of documents containing personal data are stored in Centurio and in Docmand.

As regards service providers, most data is kept in Europe but additional data may be avalaible to sub-processors located in third countries (see below point 16).

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients (on a *need-to-know* basis):

- Head of Administration Unit;
- Head of Unit of the staff member concerned;
- Human Resources Sector;
- Training manager in the CPVO;
- IT Unit staff members.

External recipients (on a *need-to-know* basis):

- Access to data is given to the following external online training providers: Altissia, EU Learn Portal, LinkedIn and their sub-processors.

15. * Period of retention for the data:

As regards personal data held in the files of staff members by the CPVO, in accordance with CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, all personal data will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

As regards data processed by the training companies, these have their own periods of retention (please refer directly to their respective privacy statements as mentioned in point 12).

16. * Proposed transfers of data to third countries or international organizations and safeguards in place, if such is the case:

The external training provider Altissia transfers data to the following sub-processors located in countries outside the EU/EEA:

- Vero (getvero.com) in Australia, with which Altissia has secured a DPA that includes Standard Contractual Clauses (or Model Clauses) approved by the European Commission with Vero. Vero may also make use of Amazon AWS in United States for storage location purposes; data transferred are name, surname and email address.
- MailChimp in the the United States, with which Altissia has signed a DPA; data transferred are only e-mail addresses;
- LearnCube in UK; data transferred are username, name and surname of the data subject;

Other important information:

LinkedIn's data centres are located in United States and transfers of data are governed by Standard Contractual Clauses approved by the European Commission; additional data may be available to further sub-processors in third countries.

17. * Measures to ensure security of processing:

At the CPVO, access to staff members applications for training courses in Centurio is restricted to the Head of Unit of the staff member concerned, the training manager and Human Resources sector.

As for the external online training providers, these have their own respective security measures put in place to ensure the security of data processing, which the CPVO has verified are appropriate. The Administration Unit will monitor the implementation of Regulation (EU) 2018/1725 as regards the organisational and technical security measures adopted by the sub-processors.

Additionally, the CPVO has ensured that an extra layer of security measures is in force in what concerns online trainings provided by LinkedIn in its Learning portal: an anonymised e-mail address (alias) is used for the training purpose (granting of a license) to avoid the identification and link with the main LinkedIn account (professional network).

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[1]

1. Name of processing:

Telework

2. * Last update of this record:

23/03/2021

3. Reference Number:

No 67

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processor:

SYSPER 2 (European Commission)

7. Description of the processing operation:

The processing operation is necessary for the implementation of the possibility for CPVO staff members to telework. In accordance with the CPVO Implementing Rules on Teleworking, a teleworking agreement can be concluded between the teleworker and his/her Head of Unit. Teleworking is an alternative working arrangement to enable the CPVO staff member availing him/herself of this possibility a better work-life balance, greater empowerment and stress reduction in stress, greater motivation leading to better performance and shorter travelling times resulting in less pollution.

The processing operation concerning telework takes place under the TIM module of SYSPER, the module relating to Time Management. SYSPER is a software created and managed by the European Commission, of which the CPVO makes use. SYSPER requires the processing of personal data in connection with the personal file of each staff member. As described in Record No 68 SYSPER, SYSPER is divided into several modules, dealing with all elements of a staff personal file (mainly CAR (Career), PER (Personal Data), FAM (Family Data) and TIM (Time Management)).

Requests for telework (*ad hoc* or structural) are made through the SYSPER TIM module and require the approval by the concerned Head of Unit of the staff member. These requests are also accessible to members of the Human Resources sector.

8. * Purpose(s) of the processing and legal basis:

Concerning general data already kept in the personal file of the teleworker, the purpose of the processing is to identify the teleworker. Personal data is obtained from the teleworker in order to enter into the Teleworking Agreement.

Legal Instruments:

- Article 1e (3) and Article 20 of the Staff Regulations of Officials;
- Article 16 of the Conditions of Employment of Other Servants of the European Communities (CEOS);
- CPVO Decision of 15 February 2019 on Working Time;
- CPVO Decision of 9 March 2021 on Telework from outside the place of employment;
- Contractual arrangement between the teleworker and the Hierarchical Superior (Teleworking agreement).

Legal Basis:

Article 5.1 (a) of the Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Only CPVO staff or staff seconded to the CPVO (officials, temporary agents, seconded national experts and contract and local staff, management included).

Teleworking is voluntary and reserved only to staff whose duties are suitable for teleworking.

10. When and how were data subjects informed:

A Privacy Statement is made available to data subjects in the intranet of the Office, Sharepoint, Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

A part of the data being processed for this operation is pre-existing in SYSPER (please refer to Record No 68 SYSPER):
- Name, surname, Personal Id and Personal Number (NUP) of the staff member;
- The percentage of occupation of post (full or part-time);
- The Unit, sector and line manager of the staff member.

As concerns particularly the teleworking activity, data subjects must provide in their request the period and the reason for requesting telework, as well as the home and/or telework location address along with a professional telephone number contact.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The Data Subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation 2015/1725 (EU) by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request. The CPVO has put in place an Internal Procedure to be followed by the CPVO Controllers in relation to Rights exercised by data subjects in accordance with Regulation 2018/1725 dated 20 March 2021.

13. Storage media of the data:

Please refer to Record No 68 SYSPER.

14. The recipients or categories of recipients to whom the data might be disclosed:

- The staff member requesting telework;
- The Head of Unit of the staff member;
- The Human Resources sector.

15. * Period of retention for the data: The data concerning the history of telework requests is kept in SYSPER as long as the staff member is in active service according to the rules of the Commission on retention of such an information. Please refer to Record No 68 SYSPER.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: The personal data is not intended to be transferred to any third country or international organization.
17. * Measures to ensure security of processing: The measures in place to ensure the security of processing are those concerning SYSPER, please refer to Record No 68 SYSPER.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controllers declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVIES[1]

1. Name of processing:

SYSPER

2. * Last update of this record:

13/04/2021

3. Reference Number:

No 68

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Administration Unit (Human Resources sector)

External processor:

SYSPER 2 (European Commission)
DG DIGIT (European Commission)
PayMaster Office (PMO) (European Commission)

7. Description of the processing operation:

Since November 2017, the CPVO avails itself of the services of SYSPER 2, an IT tool provided by the European Commission, with the aim of supporting the management of Human Resources processes and to ensure that personal data is kept adequately and rapidly retrievable. SYSPER 2 has different basic and optional modules. The CPVO currently adopts and applies the following modules:

- PER (Personal data management): it allows the management of personal data of employees, address declaration and associated validation workflow;

- ORG (Organization Chart): it enables the management of the organisational structure and management functions;

- FAM (Individual rights): it allows the management of data of staff members and family members;

- TIM (Time Management): it is the integrated solution for the management of working time and working formulas. It includes the management of absences and leaves, work patterns (e.g. part-time, parental and family leave), the recording of presences and teleworking;

- DOC (Document Management): it allows the generation and management of documents (e.g. certificates);

- JIS (Job Information System): it allows the management of job descriptions;

- CAR (Career and Mobility): it covers basic procedures for daily management of various types of staff, from the entry into service and the probation period, to mobility and interruption of the service;

- DOT (Job quotas): it enables the management and accounting of job quotas;

- STAGE (Probation reports, added in March 2021): it enables the management of the workflow of probation reports;

- VAC (Vacancies): it allows the publication of jobs at the CPVO. It covers the publication of the vacancy notice, the registration of candidates as well as the selection procedure up until the selection of the new jobholder; it is adopted just in specific circumstances.

- COMREF/RETO (Identity Management): it permits the management of profiles and use of EU platforms;

The CPVO will soon implement:

- ETHICS: it covers the management of specific declarations and requests, as requests for external activities declarations on conflict of interests and hospitality declarations;

- EVAL: it enables the management of the yearly appraisal exercise.

The CPVO HR sector and DG HR, DG DIGIT and PMO collect and use personal data to support and facilitate the management of staff and workforce (e.g. recruitments, career, appraisal, promotion, mobility, etc.) in SYSPER. For each specific process there is a specific privacy statements (please see point 12).

8. * Purpose(s) of the processing and legal basis:

The purpose of processing is to allow the determination of financial benefits and expenses payable to CPVO staff members, seconded national experts employed by the CPVO, candidates and external experts. The personal data is not used for an automated decision-making including profiling.

Legal instruments:

- Staff Regulations of Officials;
- The Conditions of Employment of Other Servants (CEOS);
- Rules on the secondment of national experts to the CPVO;
- Service Level Agreement (SLA) between the CPVO and the European Commission (Ref. Ares 229066 – 02/05/2020).

Legal bases:

- Article 5.1 (a) of the Regulation 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);
- Article 5.1 (b) of the Regulation 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

The categories of data subjects involved in the present processing operations are:

- CPVO Staff members (Officials, Temporary and Contract agents) who are subject to the Staff Regulations of Officials and the Conditions of Employment of Other Servants (CEOS) as well as high-level public office holders of the CPVO who are subject to regulation 2016/300 (where applicable);
- Staff members' family members (when applicable);
- Candidates and external experts taking part in events organised by the CPVO;
- Other external contractors involved into the CPVO's activities through their professional activity, directly or indirectly, but collaborate in the context of an employment contract with the CPVO, such as, for instance, Seconded National Experts and Trainees.

10. When and how were data subjects were informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section. Specific privacy statements relating to the single modules, respectively, are also available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

The Privacy Statement on SYSPER 2 issued by the Commission is included in the online tool and accessible on the homepage of SYSPER, before gaining access into it.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The processing operation involves the following data:

- As for the CPVO staff members: Surname, first name, status, nationality or nationalities and any change of nationality, gender, e-mail address, current and previous place(s) of residence as well as any other change of residence, study curriculum, employment curriculum, officially recognized registered partnership, identity and date of birth of spouse or partner, place of residence and any change of members including name, date of birth, nationality, place of residence any change of residence and the nature of their relationship to the staff member or high-level public office holder of the client insofar as necessary for the determination of financial benefits, data confirming the identity of former staff members and former high-level public office holders of the CPVO insofar as they are necessary for the determination of financial benefits (e.g. reimbursement of medical expenses, granting of allowances or cost reimbursement) related to the health situation; financial data needed for the payment of the different financial benefits, including identification of the bank account, the bank account holder and the bank; identity and date of birth of dependent children and date of adoption if relevant; Personal Identification Number, CPVO Unit and/or Service to which the jobholder is assigned (including job number), category, grade, status, duration of contract, years of service, unique payroll number (NUP), administrative status and career, job description; daily presence, data on contribution to pension scheme (part-time working in preparation for retirement), and information on absences: sick leave (with or without a medical certificate), special leave, annual leave, parental and family leave, and the results of calculations, particularly regarding the balance of entitlements (balance of absences, leave, parental and family leave entitlement, time credit purchased);

- Regarding trainees: name, surname, e-mail address, date and place of birth, nationality, place of residence and any change of such, official recognized partnership (if any), recording of requests and grant of leaves and period of duration of the granted leave;

- As for seconded national experts, data confirming their identity, including name, date of birth, nationality, place of residence, national employment situation, recording of requests and grant of leaves and period of duration of the granted leave; banking information (where applicable);

- As for candidates and external experts, data confirming the identity of candidates and external experts, including name, date of birth, nationality, place of residence, financial data needed for the payment of the different financial benefits, including identification of the bank account, the bank account holder and the bank;

- Logs of staff members to SYSPER (only the service provider).

In case of absences for health reasons (with or without medical certificate) and in case of special leave, SYSPER 2 does not process direct medical data of the CPVO Staff Member or his/her family members, just administrative data related to the absence. Medical diagnosis data are only processed by the medical service providers of the CPVO. For more information, please refer to Record No 10 Pre-employment and Medical Annual Visits.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Article 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit to the email address dpc@cpvo.europa.eu by *explicitly* specifying *the request*.

13. Storage media of data:

As for the CPVO, data are stored within internal servers located in the premises of the Office.

As for the external processor, data are stored on SYSPER servers of the European Commission, managed by DG DIGIT. According to the Annex 3 (Data protection) of the SLA between the CPVO and the Commission, data shall only be held in data centres located within the territory of the EU/EEA.

Furthermore, the service provider may not change the location of data processing without the prior written authorisation of the client.

14. The recipients or categories of recipients to whom the data might be disclosed:

Access to the personal data is provided to the CPVO and Commission Staff responsible for carrying out this processing operation and authorised persons according to the "need to know" principle. Such persons are bound by their statutory obligations under the Staff Regulations, and when required additional confidentiality agreement.

Internal recipients:

- CPVO Human Resources Sector;
- CPVO President, Vice-president and Heads of Unit (Senior and Middle Management);
- Other CPVO Staff members (recipients vary in relation to the specific processing activity).

External recipients:

- DG HR (European Commission);
- DG DIGIT services in view of authenticating staff members when they connect to internal databases from the outside (via external access) or when they request to switch their professional line;
- PayMaster Office (PMO) (European Commission);
- For the purposes of maintenance of the SYSPER 2 tool IT Professionals of DIGIT (European Commission);
- For the purpose of investigation and audit control, authorised staff of the following institutions may have access to relevant personal data: EU Court of Auditors, Internal Audit Service of the European Commission, European Anti-Fraud Office (OLAF);
- For the purposes of handling review procedure and litigation, access to personal data may be granted to the European Data Protection Supervisor (EDPS), the General Court, the Court of Justice of the European Union (CJEU), only to the extent necessary for handling the review procedure and litigation.

15. * Period of retention for the data:

CPVO:

In SYSPER different processing operations are carried out, with different retention periods. For the detailed retention periods, please refer to the single processing operations carried out in SYSPER.

SYSPER 2 (European Commission):

Data processed in different SYSPER 2 modules (see above point 7) have different retention periods. Please refer to the specific privacy statement related to the single procedures.

Other relevant information:

The duration of processing of personal data will not exceed the period referred to in Article 18 SLA, namely the duration of validity of the SLA. Upon expiry of this period, the service provider will, at the choice of the CPVO, return, without any undue delay and in commonly agreed format, all personal data processed on behalf of the client and the copies thereof, or will, effectively delete all personal data unless the Union law requires a longer storage of personal data. The service provider will keep the personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Where all or part of the processing is sub-contracted to a third party, the service provider will pass on its obligations referred to in the SLA in writing to those parties, including sub-contractors; At the request of the CPVO, the service provider shall provide a document providing evidence of this commitment.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

In accordance with Annex 3 (data protection) of the SLA between the Commission and the CPVO on the use of SYSPER 2, the personal data are only processed within the territory of the European Union and the European Economic Area and will not leave that territory. However, any transfer of personal data under the SLA to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the Regulation (EU) 2018/1725.

17. * Measures to ensure security of processing:

CPVO:

Personal data is stored in secure IT System according to the security standards of the CPVO. System and server are password protected and require an authorised username and password to access. The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

SYSPER 2 (European Commission):

The service provider grants restricted access to its personnel only to the extent necessary for the implementation, management and monitoring of the SLA. It ensures that employees authorised to process personal data, at any stage, have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality in accordance with the provisions of Article 16 of the SLA. The service provider adopts appropriate security and organisational security measures, taking into account the risks associated with the present processing and to the nature, including:
- The pseudonymisation and encryption of personal data;
- Ability to ensure confidentiality, integrity and availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely and efficient manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Measures to protect personal data from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[1] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Equipment Management

2. * Last update of this record:

09/04/2021

3. Reference Number:

No 69

4. * Name and contact details of the Controller:

Head of the Legal, Procurement and Logistics service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Legal, Procurement and Logistics service

7. Description of the processing operation:

In accordance with the CPVO Financial Regulation, the Office shall keep inventories showing the quantity and the value of all tangible, intangible and financial assets in accordance with a model drawn up by the accounting officer of the Commission. The inventory covers all equipment of the Office (e.g.: land, buildings, plant and equipment, computer hardware, vehicles, furniture). The Office shall check that entries in the inventory correspond to the actual situation. The Inventory manager (or IT Networks manager in the case of hardware) may make requests for de-commissioning assets in order to update the inventory list of the CPVO and the balance sheet of the office.

Where a CPVO staff member becomes aware of theft or loss of CPVO assets, he/she should notify the Head of the CPVO Logistics Service with copy to their hierarchical supervisor within one working day. For small very low value and non-inventoried items, the Head of the Logistics sector may decide that no further action is necessary. In other cases, the Head of the Logistics sector will provide the detailed form to be completed by the staff member and duly validated. The form for loss or damage, should be completed in detail, explaining the circumstances of the loss or theft, a detailed description of the item and if possible the CPVO inventory number of items. When receiving the completed form for loss or damage, the Logistics sector head shall report it to the Inventory manager.

8. * Purpose(s) of the processing and legal basis:

The processing is necessary to enable the management of the inventory of the CPVO.

Legal Instruments:

- The Regulation on the financial rules applicable to the general budget of the Union No 2018/1046;
- Article 100 of the CPVO Financial Regulation of 1 July 2019;
- CPVO Procedure of 1 January 2017 on Property and Inventory Management.

Legal Basis:

Article 5(1)(a) of Regulation No 2015/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members.

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects in the intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

- The inventory list contains the physical location for each asset. Each workstation and its location is linked to a staff member. The data subject may be identified through the location of the equipment.

- Data taken from the CPVO form for theft, loss or damage to property, in particular Staff member's name and surname, item concerned, Office No/Address where the issue occurred.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation No 2018/1725 by submitting a written request to the CPVO data controller, Head of Legal, Procurement and Logistics service, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The CPVO form is stored in a locked e-file in the intranet Sharepoint to which only authorised Staff member(s) may have access.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data may be disclosed to the following recipients on a *need-to-know* basis:
- The Head of the Legal, Procurement and Logistics service;
- The hierarchical supervisor;
- The Inventory Manager.

15. * Period of retention for the data:

In accordance with Article 42(5) of the Financial Regulation and Article 21(d) of its Implementing Rules, all financial personal data and supporting documents is kept for five years from the date on which the budget authority, namely, the Administrative Council of the CPVO, grants discharge for the budgetary year to which the documents relate. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data are not intended to be transferred to a third country or international organisation.

17. * Measures to ensure security of processing: The inventory is an excel file stored in the intranet Sharepoint, with access restricted to authorized staff members, namely, the Logistic Sector, the hierarchical supervisor and the inventory manager.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Tableau

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 70

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit

7. Description of the processing operation:

To accomplish their duties, many CPVO staff members process data in the normal workflow of tasks. In certain cases, there is an electronic trace of the work carried out and the date and time at which it was done. New reporting tools allow easy analysis of such data, providing useful operational information.

Data are taken from numerous databases: PVR / EPM / *ad hoc* Excel files. These allow the production of operational and productivity reports (including individual performance indicators). Samples of productivity reports include processing of input and payment of invoices and total commitments open (RAL) by the staff member to carry out the work. Samples of operational reports are reports based on the analysis of statistics produced on the use of the internal database Variety Finder by national authoritites and further relevant parties based on Countries or identified Areas.

As a general rule, only authorised and licensed staff members may have access to the tool for consultation. However, the Management Team of the Office may authorise certain staff members - the "Tableau Desktop Users" - to create reports using Tableau Desktop (tool creating reports). The "Tableau Desktop Users" are currently eleven staff memers. Rules governing reports may be summarised as follows:

- Reports may be prepared only by a limited number of authorised staff members (the "Tableau Desktop Users");
- Reports shall be presented at global level without individual staff information and shall not aim at producing (or allowing deducting) individual performance indicators of the staff member;
- Once the report is produced, it should be validated by the interested parties, namely the staff member concerned, staff member at the origin of data, the hieracy and the IT Unit before any publication (paper or electronic based);
- For each created report, only the person making it give access for consultation.

Furthermore, as regards particularly productivity reports, when outputs and efficiency are assessed, they may only be used in a given annual assessment of a staff member only to the extent that they refer to objectives defined for the staff member concerned in a previous annual staff evaluation. The purposes of the productivity reports and individual performance indicators must be clearly defined prior to the

production of the report and agreed upon by the Management Team of the Office. The staff member concerned by the report has the possibility to comment on the report produced.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing is to allow the analysis of raw data available in the internal databases of the CPVO and to provide useful operational information to both the staff members and the hierarchy, facilitating the decision-making and evaluation processes in the Office.

Legal instruments:

- CPVO Procedure on Management and production of IT reports;
- Articles 43 of the Staff Regulations of Officials;
- Articles 15(2) and 87 of the Conditions of Employment of Other Servants (CEOS);
- Commission on general implementing provisions for Article 43 of the Staff Regulations.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All CPVO staff members, Seconded National Experts, Interim staff, Trainees.

10. When and how were data subjects informed:

The Privacy Statement is made available in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

Data collected to elaborate productivity reports (individual performance indicators) are:

- Name initials of the staff member working on a specific file;
- Date and nature of the workflow event;
- Tasks completed.

Data gathered to produce operational reports are raw data extracted from the internal databases of the CPVO. For more information about how data are used to elaborate operational reports, please refer, for instance, to Record No 23 Variety Finder.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No. 2018/1725 by submitting a written request to the CPVO data Controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying *the request.*

13. Storage media of data:

Data processed in the Tableau reporting software is also stored there in. As regards data used to elaborate operational reports, they are stored in the internal databases of the CPVO.

14. The recipients or categories of recipients to whom the data might be disclosed:

The recipients vary in relation to the presence of personal identifiable information. Data are disclosed to the recipients on a *need-to-know* basis. As regards productivity and operational reports:
- The Hieracy;
- Authorised users;
- in specific case, general public through publications on the CPVO website;

For reports where individual information of the staff member can be identified:
- The Hieracy;
- Authorised users;
- widely distributed, only upon agreement with the staff member concerned;

The IT System Administrator may access for maintenance purposes.

15. * Period of retention for the data:

In accordance with the CPVO procedure on the use of the reporting software Tableau, operational and productivity reports using global data related to the core business of the Office can be kept as long as necessary for historic archiving or management purposes. Reports allowing individual performance indicators will be destroyed after one year from the date of the end of appraisal process.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not intended to be transferred to any third country or international organization.

17. * Measures to ensure security of processing:

Only eleven authorised staff members have access to Tableau Desktop. Such access may only be granted by selected staff members within the IT Unit. For each created report, only the person making it may give access for consultation. Then only a restricted number of authorised users may have access to the report. Authorised users cannot extend their right of access beyond permitted. Logs in Tableau related to the publication Reports are maintained (date at which the report was published and the Tableau Desktop User who published the report).

The storage media is only managed by the IT System Administrator, which have access through the domain administrator login.

Data are stored in internal databases of the CPVO. Data needed to produce individual reports are extracted from databases only by authorised users through licenses. Access to Tableau Server is limited for consultation. The access is also restricted by the use of firewalls (network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules) and the network security scheme (including a DMZ).

Personal data are only processed internally. The organisational structure includes defined responsibilities for the various aspects of data protection.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

Issuance of Laissez-Passer

2. * Last update of this record:

12/03/2021

3. Reference Number:

No 71

4. * Name and contact details of the Controllers:

Joint Controllers:

- Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

- European Commission, General Human Resources and Security, Unit HR - A.3 - HR Information Systems and Reporting Sector HR.A.3.002 - Reporting Systems and User Services

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Administration Unit (Human Resources sector)

7. Description of the processing operation:

The Laissez-Passer of the European Union (EU-LP) is a travel document granted to a list of officials and other servants of the Union and, since the adoption of Regulation 1417/2013, to certain new categories of special applicants namely family members of Members of an institution, family members of officials and of other servants of the Union who fulfil the conditions laid down in Article 23 of Staff Regulations of Officials and Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS), the officials and other servants of the Union who do not fulfil the conditions laid down in the above referred articles as well as their family members, the Seconded National Experts and their family members, the junior professionals in Delegation (JPD) and their family.

The Council Regulation 1417/2013 of 17 December 2013 lays down a new form of LP (travel document) issued by the European Union, replacing Regulation (ECSC, EEC, Euratom) No 1826/69 ("EU-LP Regulation"). It requires to the Commission to act as coordinator notably for processing purposes and to ensure compliance with Regulation (EU) 2018/1725. Regulation No 1417/2013 which indicates that the new LP should comply with the security standards and technical specifications applicable to the national travel documents issued by Member States pursuant EU legislation and keeping compliant with the specifications of the International Civil Aviation Organisation (ICAO). This includes that common security standards and interoperable biometric identifiers should be integrated into the EU-LP in addition to the biographical data.

The first phase of the enrolment (capture of personal data both biographical and biometrical (facial image and fingerprints) is covered by the provision of Article 2(1) EU-LP Regulation: "For the purpose of this Regulation each institution may conclude agreements with other institutions with a view of creating synergies and alleviating the costs". In this context it has been agreed that the European Commission would act on behalf of all other institutions/agencies.

CPVO signed a SLA with the Commission for the issue of the EU-LP for CPVO staff.
The Commission runs two locations of the enrolment stations, one in Brussels and one in Luxembourg and support the running of the European Central Bank (ECB) centre in Frankfurt.

Regarding the pre-enrolment phase, the CPVO is in charge of this phase and in this regard collects biographical data of the CPVO EU-LP applicants necessary to establish the EU-LP. The list of the biographical data collected is presented in Annex I to the EU-LP Regulation. The CPVO then sends those data to the Commission LP central service in Brussels for it to process them (integrate them into the system that will eventually encrypt them). The Commission then proceeds to process the biographical data of the applicants received from CPVO. Once the Application and delivery form is received back from the Commission LP central service, it is stored in the personal file.

The application form used to sustain the whole process of LP issuance is filled in manually within CPVO and transmitted electronically (encrypted and digitally signed) and on paper to the LP service run by the Commission (by valise/DHR).

The Commission collects (in Brussels and in Luxembourg LP Central Service) the biometrical data of the applicants, except for those captured by the ECB centre, where it is operated by the ECB but as a part of an overall unique system. Biometric data are captured during enrolment with the physical presence of the data subject.

For the two other steps of the issuance process, production of the LP and its personalisation, the EU-LP Regulation establishes that the Commission shall designate an entity to be responsible "taking due account of the sensitive nature of the documents to be produced" and in accordance with the provisions applicable to the award of contracts. Finally, once personalised, the LP are sent back to the Commission which check their quality and readability and ensures the delivery of each of them hand by hand or through remote delivery to the final holder.

The Commission processes the biometrical data of the applicants once received encrypted and via secure link. In a certain number of cases, the enrolment will take place using a mobile station able to be transported abroad, to be used by EU Agencies in Europe or by EU Delegations in the world. This will be limited to the minimum. The biometrical data will be then exported on a secure USB key and brought back to the Commission LP Central Service for further processing. The Commission then verifies the correctness and quality of the personal data collected, prepares the data in files ready to be used in the personalisation of the LP and proceeds to their encryption.

The Commission sends the encrypted biometrical and biographical data of the CPVO applicants to the external contractor for further processing (personalisation of a blank booklet/LP with those data). The Commission receives the personalised LP and checks the correctness of the document. This includes a check of the correctness of the personal data included on the vision page as well as in the clip (facial image and finger prints).

The Commission stores the personalised LP during the necessary period before delivery (normally few days but a maximum of 3 months may apply).

In case of hand-to-hand delivery, the Commission during the delivery redoes together with the applicant a check of the correctness of the data included whether visible or not (stored in the LP chip) with the exception of the fingerprints no longer accessible.

In case of remote delivery (taking place outside the Commission LP Central Service in Brussels or in Luxembourg) this operation is done only on the visible data by the Institution / Agency of origin. The remote delivery is considered an exception to the system. It includes the possibility that this remote delivery be operated outside the European borders, in the office of EU delegations situated in third countries. Remote delivery might become nevertheless the normal way for the Agencies, bodies and joint undertakings not located in Brussels or in Luxembourg.

The Commission exchanges information on the progress of the application via the exchange/transmission/reception of the application form which contains the biographical data collected and information related in some cases to the members of the family of the applicants.

The Commission is likely to be responsible for keeping the paper version of the finalised application form once the process of delivery has ended.

The Commission will liaise with the different Institutions /Agencies in charge of managing the lost and stolen LP to that end it will communicate non personal data unless a specific need appears or in case of urgency. This may include that the data subject is not informed or has not his consent collected beforehand. This may occur in case his/her own security is at stake.

8. * Purpose(s) of the processing and legal basis:

The purpose of the processing of the personal data is to allow the issuance of EU LP in accordance with the international recommendations and the European legislation, as in Council Regulation 1417/2013.

Legal Instruments:

- Council Regulation (EU) No 1417/2013 of 17 December 2013 laying down the form of the EU LP;
- Service Level Agreement (SLA) on the issuance of the laissez-passer issued by the European Union in accordance with Council Regulation (EU) No 1417/2013;
- Article 6 of the Protocol No 7 on the Privileges and Immunities;
- Article 23 of the Staff Regulations of Officials;
- Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS).

Legal Bases:

- Article 5(1)(a) (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body);

- Article 10(2)(g) of the Regulation (EU) 2018/1725 (the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject).

9. * Description of the category(ies) of data subject(s):

CPVO statutory staff and/or certain categories of special applicants according to Regulation No 1417/2013 who could request an EU-LP:

- Members of the CPVO Management Team;
- CPVO staff members who are supposed to travel regularly outside the European Union;
- Family members of CPVO Officials and of other staff members who fulfil the conditions laid down in Article 23 of the Staff Regulations of Officials and Articles 11 and 81 of the CEOS.

10. When and how were data subjects informed:

The Privacy Statement is made available to data subjects in the Intranet of the Office, Sharepoint, under the Data Protection Officer section.

The European Commission has also published a Privacy Statement on the EU-LP procedure, made available to data subjects in the DPO section of the Commission, accessible at: http://ec.europa.eu/dpo-register/detail/DPO-2318-5.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected:

- Contact information including, name and surname, date and place of birth, nationality and gender;
- Staff type, job information including assignment, job types, position, job titles, statutory link, external transfers or mobility, posting/address;
- Family position including the information for each family member applying for a laissez-passer in connection with an application for or the holding of a laissez-passer by the original holder. In particular: surname, name, date of birth, nationality, gender, address, link with the original holder.

Detailed data included in each personalised laissez-passer may differ following the specific requirements inherent to each demand, in particular the position in the diplomatic list of mentions.
Biometrical personal data: facial image, fingerprints and signature of the holder.
Data concerning fingerprints are not processed for children under 12 years old.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subject has the right to access, rectify, block, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit by *explicitly* specifying *the request* at dpc@cpvo.europa.eu; or to the Commission, Directorate - General Human Resources and Security, Unit HR - A.3 - HR Information Systems and Reporting Sector HR.A.3.002 - Reporting Systems and User Services.

13. Storage media of data:

CPVO stores the data in the personal files . Hard copies are stored in a locked cupboard. Electronic personal files are stored in the internal IT tool Docman.

The Commission stores both biometrical and biographical data in the LP service run by the Commission for the steps under its responsibility for both paper and electronic versions. The Commission is responsible for keeping the paper version of the finalised application form once the process of delivery has ended.

14. The recipients or categories of recipients to whom the data might be disclosed:

- CPVO authorized staff of the HR Sector;
- The Commission LP central service in Brussels and in Luxembourg and authorized staff in Frankfurt;
- National authorities responsible for the border control;
- The authorities in charge of security at the border including airports, maritime or fluvial ports;
- The national authority responsible for the management and lost and/or stolen document, including those of non EU countries;
- The Appointing Authority (AA) and the Authority Authorized to Conclude Contracts (AACC);
- The disciplinary bodies in the institution, notably IDOC; OLAF;
- The auditors, Interpol, SIS II, Sirene; Europol, Cepol;
- The central alert system 24/7 within the remit of its competencies, on a *need-to-know* basis.

15. * Period of retention for the data:

Independently of the purpose of the EU-LP process, each Institution/Agency stores the personal biographical personal data of its applicants and special applicants according to their own rules.

In accordance with the CPVO Decision of 31 March 2021 on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members, the biographical data and the application form collected by CPVO will be destroyed after a period of 10 years from the date of the end of contract of the staff member.

CPVO will keep a scanned copy of the application form for the period of validity of the EU-LP. The original form of CPVO applicants will be kept by the Commission EU LP central service. Within the first year a scanned version of the paper version is done and electronically stored in a database managed by the Commission LP central service for the remaining period of validity of the LP.

Fingerprints and digital signature are stored only for the time necessary to the effective and successfully delivery of the LP. They are deleted at that time (a few days depending on the day the future holder takes to come and collect the personalised document with a maximum of 3 months). The LP is destroyed if not delivered. Nevertheless, they remain stored in the chip contained into the LP under the responsibility of the holder including for their submission to the controls operated at the borders.

Biometrical personal data: The retention should be limited to the need for all holders (normal and/or special applicants as well as ad hoc holders):

- Facial image, fingerprints and digital signature at the level of the contractor: the retention period is limited to the time needed to issue the EU LP after successful validation and fulfilment of the acceptance process (normally a few days and up to a maximum of 3 months);

- Fingerprints and digital signature at the level of the Commission: The retention period is limited to the time needed to issue the EU LP after successful validation and fulfilment of the acceptance process (a few days and up to a maximum of 3 months);

- For facial image at the level of the Commission: the retention period is limited to the time needed to issue the EU LP (maximum 6 years).

At the expiration of the validity of the EU LP, the LP must be returned to the Commission to be cancelled and/or partially or totally destroyed. After this process, in case it is cancelled but not totally destroyed, it may be kept by the holder. In this later case, the data (both biographical and biometrical) continue to be accessible on the invalid LP under the sole responsibility of the holder. Access to biometrics would nevertheless continue to depend on the use of specific technical devices not commercially easily accessible.
16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case: There are no proposed transfers of data to third countries or international organizations.
17. * Measures to ensure security of processing: The management of the personal data within the issuance process will be submitted to specific secure rules taking into account the ICAO recommendations and the EU legislation for EU national passports and other travel documents including EU LP. CPVO IT security measures apply to the personal data processed in CPVO. All persons dealing with personal data in the context of the IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement. Only encrypted email are sent to LP service of the Commission.
18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

E-Recruitment

2. * Last update of this record:

22/03/2021

3. Reference Number:

No 72

4. * Name and contact details of the Controller:

Head of Administration Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Name and contact details of the processor:

Internal processor:

Administration Unit (Human Resources sector)

External processors:

Kioskemploi and its sub-processors

7. Description of the processing operation:

Candidates can have access to the employment offers published on the CPVO website (through GestMax tool) and to his/her "account" (or "my CV"). The candidate should fill in and validate his/her application by confirmation from his/her mailbox. Once the applicant submits the filled in application form, an automatic acknowledgement of receipt is sent by the tool to the candidate. Candidates have the means to delete or modify their personal data themselves.

Once the call has closed, Human Resources staff members screen the candidates for eligibility. In what concerns traineeships, the Selection Committee members consult the applications of the eligible candidates and determine a list of candidates to invite to interview. Human Resources staff will then proceed to invite these candidates to interview through GestMax, and notify the Selection Committee of the interview schedule. The Selection Committee subsequently informs Human Resources of the outcome of the interview, and Human Resources informs the applicants through GestMax about the outcome of the selection procedure (application not withheld, job offer).

As regards fixed posts, the Selection Committee members consult the applications of the eligible candidates in GestMax. They determine a list of candidates to invite to interview (and a possible written test) according to a pre-defined pre-evaluation grid. A final evaluation grid with thresholds is previously established in GestMax for the interview and test. After the interviews and tests have been completed, the Selection Committee fills out the scores and comments in the evaluation grid for each candidate, and establishes a shortlist in order of merit. Minutes of all Selection Committee meetings are kept in a recruitment file on SharePoint with restricted access.

The shortlist drafted by the Selection Committee is then proposed to the President, who takes the final decision on the recruitment procedure: to offer a post and/or establish a reserve list or to close the call as unsuccessful. The decision of the President is prepared manually by Human Resources sector, who also informs the Selection Committee of the decision taken. Applicants are informed by e-mail about the outcome of the selection procedure.

8. * Purpose(s) of the processing and legal basis:

The e-recruitment tool allows the Human Resources sector to manage the entire e-recruitment process electronically, from the receipt of applications to the final recruited candidate.

Legal Instruments:

- Articles 27-34 of the Staff Regulations of Officials;
- Articles 12-15 and 82-84 of the Conditions of Employment of Other Servants (CEOS) (for temporary and contract agents);
- SLA of 7 April 2016 between the CPVO and Kioskemploi.

Legal Basis:

- Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

Candidates to CPVO vacancies published on the CPVO website.

10. When and how were data subjects informed:

The Privacy Statement is made available to candidates to CPVO vacancies along with the vacancy announcement.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The application form contains the following data:
- Name and Surname;
- Birthdate and Place and Country of birth;
- Title (optional);
- Nationality;
- Telephone number;
- Postal address;
- E-mail address;
- Military situation;
- CV, including Educational background, Professional Experience, Language Knowledge, IT and soft skills;
- Motivation letter.

For those attending the interview, the following further data is processed:
- Copy of education and work certificates (this would not be sent via the CPVO online recruiting Software);
- Legal entity and financial forms (for those having the right to reimbursement of travel and accommodation costs).

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data controller, Head of Administration Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Data are kept in the e-recruitment tool and processed through GestMax+ platform (combining a database and servers serving up HTML pages). Data are stored within the European Union.

14. The recipients or categories of recipients to whom the data might be disclosed:

Data can be accessed by the following recipients on a *need-to-know* basis:

Internal recipients:

- Members of the Human Resources sector staff in charge of processing the applications, the Management of the CPVO, the Selection Committee members and, in case of recruitment, the Accounting & Finance sector. Internal and external auditors may as well access the data if necessary.

External recipients:

- Kioskemploi and its sub-processors.

15. * Period of retention for the data:

In accordance with the CPVO Decision on retention period for personal data of candidates in CPVO recruitment procedures and for personal data in the files of CPVO staff members of 31 March 2021, data from unsuccessful candidates kept on paper or in electronic format will be destroyed after a period of 2 years from the date of decision of the Office appointing the successful candidate and, as regards successful candidates, data are kept in the personal files and destroyed after a period of 10 years from the date of the end of the contract of the staff member.

Regarding those working documents, in paper or electronic format, that are used by the members of the Selection Committee for recruitment procedures in the CPVO, these are destroyed once the selection procedure is closed, that is, on the date of the decision of the CPVO appointing the successful candidate.

As regards data processed by the external service provider Kioskemploi and its sub-processors, data are retained for no more than two years from the end of the selection procedure.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

The personal data is not transferred to any third country or international organization.

17. * Measures to ensure security of processing:

Access to GestMax is usename- and password-protected, and is accessible only to the Human Resources sector staff members as well as to authorised staff members participating in the recruitment procedure.

Kioskemploi and its sub-processors implement appropriate technical and organisational measures, in order to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Measures are in place to protect the confidentiality of the data stored on the service provider's platform GestMax.

Only authorised staff members of Kioskemploi and Kioskempoli sub-processors may access remotely the servers and the data. Access to servers of Kioskemploi are secured and protected by a firewall. Kioskemploi monitors on a daily basis any flaws identified in the tools in place and conducts as well a more comprehensive review a few times per year.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES[i]

1. Name of processing:

CPVO Online Application System

2. * Last update of this record:

30/03/2021

3. Reference Number:

No 73

4. * Name and contact details of the Controller:

Head of Technical Unit
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Technical Unit

7. Description of the processing operation:

In order to be able to use CPVO online application system and file an application for a plant variety right, an applicant needs to create a user account via CPVO Extranet:

- If the applicant is already a client to the CPVO, he/she should have a login and password;
- If the applicant is a new applicant, he/she can create a temporary account ("Create an account") and file his application;
- If an applicant is residing outside the European Union, he/she has to appoint a procedural representative based in the European Union to file the application for him.

Through the user area, access is provided to CPVO Variety Finder and CPVO online application system (MyPVR) for plant variety rights. Once user account is created, in order to enter CPVO online application system area, the "Terms and Conditions concerning electronic systems communication with and by the Office as established in decision of the President of the CPVO" need to be read and accepted.

Data collected are stored in the internal server of the CPVO PVR, and processed by authorised staff members in order to carry out the relevant operations. The requested data for filling in the application is described in point 11.

8. * Purpose(s) of the processing and legal basis:

The purpose is to process the applications for Community Plant Variety rights and exchange of information in relation to applications with users/applicants.

Legal Instruments:

- Articles 50, 87, 88 and 89 of Regulation (EC) No 2100/94;
- Articles 2 and 6 of Regulation (EC) 874/2009.
- CPVO Procedure of 20 January 2020: Reception procedure.

Legal Bases:

- Article 5.1 (a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- Article 5.1 (b) of Regulation (EU) 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject).

9. * Description of the category(ies) of data subject(s):

Users of CPVO online application system including applicants for Community Plant Variety Rights, as well as Procedural representatives and breeders.

10. When and how were data subjects informed:

Data subjects, when registering as new users are required to accept the "Terms and Conditions concerning electronic systems of communication with and by the CPVO established in Decision of the President of the Office concerning electronic communication with and by the Office". This document is published on the CPVO website. A privacy statement is also published on the CPVO website.

11. * Description of the data or categories of data:

The requested data in the application form for a Community Plant Variety right are the following:

- Applicants' Name and Surname;
- Official postal address (post code, cuty, country);
- Telephone (optional);
- Fax (optional),
- Email (An e-mail address is compulsory: if data subject is a party to proceedings; also if it is the officially registered correspondence address; if an applicant have not appointed a representative; if, in case of co-applicants, the data subject is the first named applicant and based in the EU).
- If there are any Procedural representative: his/her Name and Surname, address, address for correspondence if it is different from official address, post code, city, country, email;
- Name and Surname, and postal address of the breeder (natural person);
- Further data relating to the application for a CPVR, including botanical taxon and designation of the variety;
- Details of all other applications for plant variety rights or official variety lists concerning the variety for which protection is sought;
- Information concerning priority.

Optionally, a proof of payment may be uploaded and further data might be disclosed.

12. Procedures to grant data subjects rights (rights of access, to rectify, to block, to erase, to object):

The data subjects rights are foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) No 2018/1725. The Data Subject has the right to access his data any time by logging to CPVO online application system. In other cases a written request should be submitted to the CPVO data Controller, Head of Technical Unit, at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

The application containing personal data, once received, is automatically stored in the internal database of the CPVO "PVR". Documents are also stored in the internal database Docman.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

Data collected are processed only by the staff responsible of the corresponding processing operations on the basis of the *need-to-know* principle.

External recipients:

Personal data contained in certified applications for CPVR as well as titles granted may be transferred to Examination Offices responsible for the DUS examination of the candidate variety. Furthermore, for

reasons of public interest some data are also published on the CPVO Gazette and on the website of the Publications Office of the European Union. For more information, please see Record No 16 Cooperation with Examination Offices and Record No 11 Publications.

15. * Period of retention for the data:

In accordance with Article 2 of the "Decision of the President of the Office on the form of Registers kept by the Office, retention and the keeping of files including documentary evidence, publication of the Official Gazette", in case a title is granted, data will be kept for a period of 30 years from the expiry of the granted Community plant variety right.

Otherwise, it will be kept for a period of 10 years following the date of rejecting the application or the date of the withdrawal of the application or the date on which the Office informs the applicant that the Office considers the application abandoned.

16. * Proposed transfers of data to third countries or international organizations and safeguards if such is the case:

In accordance with Article 89 of Regulation (EC) 2100/94, the CPVO publishes on a monthly basis updates referring to new applications received as well as titles granted. These data are also published in the website of the Publication Office of the European Union. The relevant data contained in certified applications and titles granted may be available to the general public for public interest purposes.

17. * Measures to ensure security of processing:

The CPVO has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into account the risk presented by the processing and the nature of the personal data processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purpose of this processing operation.

All persons dealing with personal data in the context of IT systems, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.

Access to Docman is username- and password-protected and only the concerned recipients on a *need-to-know* basis have access to documents relevant to the procedure. In addition to the access rights granted to selected recipients, Docman may be accessed only by CPVO/users from the internal network (on premises) or through the remote VPN SSL.

Access to the online application system is provided only to registered users, and is username- and password-protected.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

[i] The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.

CPVO
Community Plant Variety Office

RECORD OF PROCESSING ACTIVITIES

1. Name of processing:

Visitors Register

2. * Last update of this record:

17/03/2021

3. Reference Number:

No 74

4. * Name and contact details of the Controller:

Head of Legal, Procurement and Logistics service
E-mail address: dpc@cpvo.europa.eu

5. * Name and contact details of DPO:

Ms Gloria Folguera Ventura
E-mail address: dpo@cpvo.europa.eu

6. Service responsible for processing personal data:

Internal processor:

Legal, Procurement and Logistic Service

External processor:

Challancin Group (security services)

7. Description of the processing operation:

The processing operation concerns the management of visitor accesses to the CPVO. Visitors accessing the CPVO premises should register their presence directly at the Reception located in the main building of the CPVO (building in Boulevard Foch 3, Angers, France). Following the registration, visitors are provided with a badge and accompanied by a security guard to the concerned building. The register of visitors is kept in paper, and includes the date and time of arrival and departure.

8. * Purpose(s) of the processing and legal basis:

The purpose of processing personal data is to avoid unauthorised individuals from entering the CPVO installations, as well as tp ensure the security and safety of CPVO visitors, installations, systems and patrimony of the Office.

Legal instruments:

- Article 30 of the Council Regulation (EC) No 2100/94 on Community plant variety rights.
- CPVO Decision on the use and retention period of personal data visitors shall disclose in the entrance register in order to gain access to the CPVO premises.

Legal Basis:

Article 5.1 (a) of Regulation (EU) No 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

9. * Description of the category(ies) of data subject(s):

All persons having an authorisation to enter the CPVO premises, including: staff members, members and observers of the Administrative Council of the CPVO, Seconded National Experts, trainees, external contractors, service providers, visitors, event attendees, students, retired employees, and partners.

10. When and how were data subjects informed:

The Privacy Statement, in both English and French language, is made available to data subjects at the Reception of the CPVO for consultation.

11. * Description of the data or categories of data (including, if applicable, special categories of data (Article 10) and/or origin of data):

The following data are collected:

- Name, surname,and signature of the visitor;
- Name of the staff member with whom the visitor has the appointment;
- Date, arrival and departure times.

12. Procedures to grant data subjects rights (rights of access, to rectify, to restrict, to erase, to object):

The data subject has also the right to access, rectify, restrict, object and erase his/her personal data in the cases foreseen by Articles 17, 18, 19, 20, 21 and 23 of Regulation (EU) 2018/1725 by submitting a written request to the CPVO data Controller, Head of Legal service at dpc@cpvo.europa.eu, by *explicitly* specifying the object of the request.

13. Storage media of data:

Paper copies are kept in a locked cupboard under the supervision of the security guard.

14. The recipients or categories of recipients to whom the data might be disclosed:

Internal recipients:

- Authorised CPVO staff members;

External recipients:

- Security guards and responsible CPVO staff members.

15. * Period of retention for the data:

Data will be retained for a period of six months. At the the end of retention period, paper copies will be destroyed by the Procurement and Logistic sector.

16. * Proposed transfers of data to third countries or international organizations and safeguards in place if such is the case:

There are no proposed transfers of data to third countries or international organizations.

17. * Measures to ensure security of processing:

Paper documents are locked in safe cupboards. All the recipients signed a confidentiality declaration.

18. * For more information, including how the data subject exercises his/her rights to access, rectification, object and data portability (where applicable), see the privacy statement.

The fields marked with * are mandatory

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer.