EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR EUROPEAN CIVIL PROTECTION AND HUMANITARIAN AID OPERATIONS (ECHO)
Emergency Response Coordination Centre
Emergency Response Operations

Brussels
ECHO.A.1/CG

PROTECTION OF YOUR PERSONAL DATA

Processing operation: Processing of personal data linked to the organisation and management of meetings and visits under the Union Civil Protection Mechanism (UCPM)

Data Controller: European Commission
Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO)
Unit A.1 – Emergency Response Operations

Record reference: DPR-EC-01063

Table of Contents

1 INTRODUCTION

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to 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.

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

This privacy statement concerns the processing operation '**Organisation and management of meetings and visits under the Union Civil Protection Mechanism (UCPM)'** undertaken by the European Commission, DG ECHO, Unit A.1 – Emergency Response Operations (hereafter 'ECHO.A.1'), as presented below.

2 WHY AND HOW DO WE PROCESS YOUR PERSONAL DATA?

Purpose of the processing operation: ECHO.A.1 collects and uses your personal information only for the organisation, preparation, management and follow-up of physical, virtual, and hybrid meetings and physical visits related to the performance of emergency operations within the framework of the UCPM.

More specifically, this concerns the following processing activities:

- communication activities such as sending e-mails and invitations (this entails the management of contact lists for correspondence);
- exchange of meeting documents, notably through information sharing and circulation of documents via email, and sharing of information with other Commission services to follow-up on the meeting concerned;
- organisational and administrative activities to ensure access to Commission buildings for meeting participants and visitors, including preparation and issuance of V-PASS (see Record DPR-EC-00655 'Commission Physical Access Control System (PACS)');
- reimbursement of travel costs (see Records DPR-EC-01141 'Information system supporting the organization of meetings' and DPR-EC-00301 'Registration of Legal Entity and Bank Account records in the central EC Accounting System);
- audio-visual recording of meeting(s) for the purpose of drafting minutes and summary records (see Record DPR-EC-03266 'Audio and Audio-visual

recording of meetings requested via the Commission's internal Room Booking system').

No personal data of individuals are included in the summary records of meetings and no personal data will be published.

Summary records of meetings and list of authorities represented at the meetings are recorded for internal purposes.

Physical access to Commission buildings and premises is subject to security measures. In order to participate in a physical visit to DG ECHO premises, you have to go through a registration process in order for a pass to be issued in your name. In practical terms, you may register by providing your personal data to ECHO.A.1. Your data will be then submitted by ECHO.A.1 to V-PASS – the Commission's in-house application for centralised and electronic management of visitor access requests. For more information, please refer to Record DPR-EC-00655.

Video-conference tools (i.e. Microsoft Teams and Webex) may be used notably as a means to facilitate remote participation to meetings. The processing operation of personal data through these tools is covered by dedicated data protection records which are included in the DPO's public register with the following references:

- DPR-EC-04966.4 'EC M365 environment'; and
- DPR-EC-05006 'Service de Web Conference (Webex)'.

Audio-visual recording(s) at the meeting of the speakers, organisers and participants may be taken for internal purposes (such as the drafting of minutes and summary records) and to share the recording(s) with UCPM Member States and Participating States unable to attend the meeting.

Participants that do not wish to be part of the above web-streaming and recording activities have the possibility to object to the processing as follows:

- They should inform the organisers by a reply to the invitation email. This may, however, impede participants and especially presenters and speakers from participating in the meeting.

- Those following the event remotely via a web conference tool may decide not to share their image, voice or messages by turning-off their cameras, muting their microphones and/or not using the chat function during the meeting.

- Those attending the meeting in person may be advised to sit in back-rows or photographs/video-free areas of the meeting room, if available.

Your personal data will not be used for any automated decision-making including profiling.

3 ON WHAT LEGAL GROUND(S) DO WE PROCESS YOUR PERSONAL DATA?

The processing operations on personal data, linked to the organisation, management, and follow-up of meetings and visits under the UCPM are necessary for the management and functioning of the Commission, as mandated by the Treaties. Those provisions are, in particular, Article 11 of the Treaty on European Union and Article 15 of the Treaty on the Functioning of the European Union. In addition, the processing operations relate to meetings and visits the organisation of which takes directly part in, or is otherwise connected with, the proper implementation of operations and activities performed in the context of the UCPM under Decision 1313/2013 of the European Parliament and of the Council of 17 December 2013, and related implementing acts.

In the event that a meeting is to be recorded, your consent to appear in the audio-visual recording and to share this recording with other UCPM Member States and Participating States is requested. You consent will also be requested for sharing the meeting participants' lists, which contains your name and organisation, with other participants. If you opt-in, you are giving us your consent under Article 5(1)(d) of Regulation (EU) 2018/1725 to process your data for this specific purpose. **You can give your consent via a clear affirmative way by a reply to the invitation email**. Your consent for these services can be **withdrawn** at any time by contacting the data controller of the meetings, as specified under Heading 9 below.

Therefore, we process your personal data because:

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 5(1)(a) of Regulation (EU) 2018/1725);

b) you have given consent to the processing of your personal data for the following specific purposes (Article 5(1)(d) of Regulation (EU) 2018/1725):

- the audio-visual recording and photographs depicting you in an identifiable way;
- the sharing of the audiovisual recording with UCPM Member States and Participating States unable to attend the meeting;
- the sharing of the meeting participants' list, which contains your name and organisation, with other participants;
- where applicable, the auto-generated sharing of the webinar participants' list, which contains your name and organisation, with other participants via Webex.

Surveys may be organised during the meetings notably to seek participants' views on the meetings or parts thereof or seek their views on the organisation of future similar meetings.

Such surveys are covered by Record DPR-EC-01011. For information about surveys conducted through EUSurvey, please refer to Record DPR-EC-01488.

Please note that you assume full responsibility for the collection and/or publication of photos, audio and visual recordings and for any other processing of personal data that you might carry out during the event at your own initiative.

4 WHICH PERSONAL DATA DO WE COLLECT AND FURTHER PROCESS?

In order to carry out this processing operation ECHO.A.1 may collect the following categories of personal data of participants:

1. **Data necessary for physical visits:**
    - personal data necessary for organising and managing visits, and for security (access control to Commission buildings): first name, last name, email address, visitor type (i.e., visitor, contractor, pensioner), nationality, date of birth, ID card/Passport number, expiry date of identification document, organisation (company/institution) of affiliation, mobile number.

2. **Data necessary for meetings:**
    - personal data necessary for organising and managing meetings: gender, first name, last name, organisation (company/institution) of affiliation, email address, phone/fax number;
    - personal data necessary for security (access control to Commission buildings): first name, last name, visitor type (i.e., visitor, contractor, pensioner), nationality, date of birth, ID card/Passport number, expiry date of identification document, , organisation (company/institution) of affiliation, email address, mobile number;
    - personal data necessary for reimbursements purposes: banking details;
    - personal data necessary for establishing the attendance list and the minutes: signature, audio-visual material, photographs of the meeting.

The provision of such personal data is mandatory in order to allow for the organisation of the meeting and visit, the access of participants to Commission buildings and their reimbursement. If you do not provide the required information, you will not be able to participate in meetings and visits, and/or to be reimbursed.

We have obtained your personal data either directly from you, via the Ministry or National Authority you work for or via the Permanent Representation of your country in Brussels.

5 HOW LONG DO WE KEEP YOUR PERSONAL DATA?

ECHO.A.1 only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for a maximum of **5 years** after closure of the administrative file of the last meeting you have attended.

This information is without prejudice to different retention periods which may apply to personal data processed for the purpose of reimbursing travel costs and ensuring the participant's access to Commission buildings based on the dedicated processing operations notified to the DPO by the responsible Commission departments (i.e. Records: DPR-EC-00655 (Commission Physical Access Control System (PACS), DPR-EC-00301 (Registration of Legal Entity and Bank Account records in the central EC Accounting System), and DPR-EC-01141 (Information system supporting the organisation of meetings).

In case of audio-visual recordings of the meetings, the recordings will be kept for **3 months** after the meeting before being deleted. More information is available in Record DPR-EC-03266 (Audio and Audio-visual recording of meetings requested via the Commission's internal Room Booking system).

User-generated information (i.e. video/audio/chat conference content, pictures, presentations) will be kept until the event ends.

Personal data shared with the Directorate-General for Human Resources and Security of the European Commission for the participants to gain access to Commission buildings is kept for **6 months** after the termination of the link between the data subject and the Commission (see DPR-EC-00655).

Personal data collected on the occasion of surveys will be kept for a maximum of **5 years**, in line with Record of DPR-EC-01011.

6 HOW DO WE PROTECT AND SAFEGUARD YOUR PERSONAL DATA?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission or of its contractors (processors), if contractors are engaged to assist the controller.

All processing operations are carried out pursuant to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security measures and guidelines, as well as Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission and Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, its implementing rules and the corresponding security notices. These documents (as adapted from time to time) are

available for consultation at the following address: Security standards applying to all European Commission information systems - European Commission (europa.eu).

In order to protect your personal data, the Commission 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 consideration the risk presented by the processing and the nature of the personal data being processed.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

The Commission's processors (contractors) are bound by a specific contractual clause for any processing operations of your personal data on behalf of the Commission. The processors have to put in place appropriate technical and organisational measures to ensure the level of security, required by the Commission.

7 WHO HAS ACCESS TO YOUR PERSONAL DATA AND TO WHOM IS IT DISCLOSED?

Access to your personal data is provided to the Commission staff authorised for carrying out this processing operation and to other authorised Commission staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The access to all personal data related to meetings and visits is User ID/Password protected and only accessible for the authorised Commission staff member(s) involved with the organisation of the meetings and visits.

More specifically, the following Commission staff have access to certain parts of the personal data:

- authorised staff of the European Commission's Directorate-General for Human Resources and Security have access to the personal data necessary for providing access to European Commission buildings;
- authorised staff of the European Commission's Directorate-General for Budget and the Paymaster Office (PMO) have access to the personal data needed for reimbursement purposes;
- authorised staff of the European Commission's Directorate-General for Interpretation (SCIC) as meeting room and equipment providers have access to the audio-visual recordings;
- authorised staff of other European Commission departments involved in the policy follow-up to a specific meeting and visit.

In the event that the meeting is taking place via Webex the following apply:

- The Contractor, CISCO International Limited, 1 Callaghan Square Cardiff, CF10 5BT, United Kingdom will be a recipient for several sets of data (Host Registration/Host Usage) for the provision and operation of the service, for statistics, performance and billing purposes.

- The controller will transfer your personal data to the following recipients in a third country (UK and USA) in accordance with Regulation (EU) 2018/1725.

Category of personal data	**Datacenter Location**
Registration Information	Germany (AWS), the Netherlands, the United Kingdom
Host and Usage Information	Germany (AWS), the Netherlands, the United Kingdom
User-Generated Information	Germany (AWS), the Netherlands, the United Kingdom

- The controller will transfer your personal data based on a procurement contract including the Standard Contractual Clauses (SCCs) among various data protection and security clauses. Supplementary measures have also been taken by both the controller and the processor (Contractor). Back-up data processed outside the European Union and the European Economic Area, are also subject to the SCCs mechanism.

- Transfers to the UK are covered by Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

- Transfers to the US are covered by the Adequacy decision for the EU-US Data Privacy Framework, where CISCO Systems, Inc. (the Contractor) is listed under the Data Privacy Framework Program, which guarantees an adequate level of protection for transfers of personal data from the EU to US via the Contractor.

In the event that the meeting is taking place via MS Teams the following apply:

- For services related to the Office 365 cloud-based collaboration platform, Microsoft acts as data processor. Contact details: Microsoft Ireland, South

County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.

- For certain limited categories of personal data which are detailed in the below scenarios, Microsoft Ireland may transfer personal data to the USA or any other country in which Microsoft or its sub-processors operate. These data flows take place from Microsoft Ireland to Microsoft Corp. in the USA and to Microsoft's sub-processors.

- Microsoft Ireland has signed with Microsoft Corp. the new Standard Contractual Clauses ("SCCs") adopted by Commission Implementing Decision (EU) 2021/914 (module three: processor-to-processor). The new Standard Contractual Clauses cover all transfer scenarios indicated below.

- Service generated data (SGD) is processed outside of the EU. In most cases, SGD is pseudonymised before being transferred (see Section 4.4 or Section 2.2 of the data protection record DPR-EC-04966 'EC M365 environment').

- **International data transfers** are effectively taking place in four transfer scenarios:

    1. SGD transfers

    SGD transfers for Combatting fraud, Cybercrime, and Cyberattacks and Compliance with Legal Obligations are protected by encryption (ensuring their confidentiality in transit).

    2. Worldwide access to EC M365 environment

    Logging into the EC M365 environment is done with the email address only. Microsoft's servers process the domain name @ec.europa.eu of the Commission redirecting to the EC M365 environment. Finally, authentication is happening via EU Login (see DPR-EC-3187).

    3. Support case

    Only designated second-level support teams (system administrators) can open support cases with Microsoft. Most support cases do not need access to 'Customer Data'. In exceptional cases where such access is needed, mitigation is achieved by activating the 'Customer Lockbox' feature. This feature enforces customer approval for giving time-bound access to any 'Customer Data' by Microsoft engineers.

4. Microsoft 365 Apps licensing and activation data

In the context of combatting software piracy, Microsoft needs to verify a user's right to use Office products and manage product keys. This process is essential for the provision of the service and cannot be avoided. The standard technical measures for securing transfers, notably robust protection against interception, apply.

Considering the specific circumstances of the transfers, the use of appropriate safeguards and the above analysed supplementary measures, the transfer of personal data concerned to the United States is effectively subject to appropriate safeguards.

Please note that pursuant to Article 3(13) of Regulation (EU) 2018/1725, public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The further processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8 WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. As regards this processing operation, you can exercise the following rights:

- the right to access your personal data (Article 17 of Regulation (EU) 2018/1725)
- the right to rectification in case your personal data is inaccurate or incomplete (Article 18 of Regulation (EU) 2018/1725);
- the right to erase your personal data (Article 19 of Regulation (EU) 2018/1725);
- where applicable, the right to restrict the processing of your personal data (Article 20 of Regulation (EU) 2018/1725);
- the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(1) on grounds relating to your particular situation; and
- the right to data portability (Article 22 of Regulation (EU) 2018/1725).

If you have consented to provide your personal data to ECHO.A.1 for the processing operations described under Heading 3 you can withdraw your consent at any time by

notifying the Data Controller, as described below. The withdrawal of your consent will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference as specified under Heading 10 below) in your request.

Any request for access to personal data will be handled within one month. Any other request mentioned above will be addressed within 15 working days.

9 CONTACT INFORMATION

The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller referring to the specific meeting/visit your communication is related to:

European Commission, DG ECHO, Unit A.1 (ECHO-A1@ec.europa.eu).

The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e., you can lodge a complaint) to the European Data Protection Supervisor (EDPS@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10 WHERE TO FIND MORE DETAILED INFORMATION?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and

notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-01063.