Data protection statement on the processing of personal data for virtual events and videoconferencing using Zoom

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to protecting your personal data and ensuring respect for data subjects' rights when performing our tasks and providing our services. All data of a personal nature that identify you directly or indirectly will be processed lawfully, fairly and with due care.

The processing operations described below are subject to the EPO Data Protection Rules (DPR).

The information in this statement is provided in accordance with Articles 16 and 17 DPR.

Zoom Video Communications (hereafter: "Zoom") is a cloud-based videoconferencing (VICO) platform that enables organising events in a virtual environment in such a way that effective interaction between participants is as close as possible to a face-to-face experience. In view of the need for the Office and its stakeholders to continue to enjoy access to all services, the EPO has extended the use of videoconferencing in order to organise virtual events.

1. What is the nature and purpose of the processing operation?

Personal data are processed in the Zoom platform for the purpose of running virtual events and ensuring effective collaboration and communication between the Office and its stakeholders (i.e. the participants to events), thus guaranteeing EPO's business operations and compliance with applicable legal obligations.

The collected data may also be used to compile anonymised statistics on the meetings and participants, such as data on the type of meeting, number of meetings, average duration, meeting interruptions and reconnections, for quality assurance and volume monitoring purposes.

In addition, Zoom may process personal data for its own 'Legitimate Business Purposes' as an independent data controller, provided that such processing is strictly necessary and proportionate and done for any of the following purposes:

a) processing data from which data subjects are directly identifiable for the purposes of billing, account and customer relationship management and associated correspondence, complying with and discharging legal obligations, detecting, preventing and protecting against abuse, for virus scanning and scanning to detect violations of terms of service; and
b) compiling pseudonymised and/or aggregated data for the purposes of improving and optimising the performance and core functionalities, internal and financial reporting, revenue and capacity planning and forecast modelling, and receiving and using feedback for overall service improvement.

As part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between meeting participants during a particular meeting or event, such as instant messages (chat), images, files, whiteboards, transcripts and recordings. Any such purposes are established by the organiser of the event.

Recordings via Zoom are done only if strictly necessary for legitimate and explicit purposes and approved in advance. The Office has configured the tool's default settings in such a way that no one can record (except with specific authorisation). The participants will be informed whenever recordings are planned and are

automatically notified when a recording starts and will be given the option to leave the virtual event if they do not wish to be recorded.

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

2. What personal data do we process?

The following categories of personal data may be processed for participants to an event, i.e. current and former EPO staff members, contractors and externals:

- contact information, such as contact details, (work) email address, phone number(s), country;
- device management data, such as MAC address, account ID, platform-specific IDs;
- browsing information, such as IP address, URL, browser type, browser user agent, cookie information;
- information about physical and / or digital identifiable assets, such as mobile device name, mobile device's network adapter MAC address, (physical or virtual) workstation hostname, workstation network adapter MAC address, operating system version;
- session and telephony session metadata;
- geolocation;
- any additional category of personal data provided voluntarily by participants during the course of exchanges, such as chat content or oral communication, answers to surveys, assessments or quizzes.

As Zoom is a collaborative tool, additional personal data may be included in the information that is exchanged between meeting participants during a particular meeting or event, such as instant messages (chat), images, files, whiteboards, transcripts and recordings (e.g. recordings of faces or voices). Any such purposes are established by the organiser on the basis of what is strictly necessary and proportionate.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the CIO of EPO's Principal Directorate, who acts as the EPO's delegated data controller.

Personal data are processed by the staff of the Productivity Apps, Collaboration & Events department for the purposes of managing the technical means to conduct virtual events.

Zoom and its third-party service providers providing service support and maintenance may also access and process personal data.

4. Who has access to your personal data and to whom are they disclosed?

Personal data are disclosed on a need-to-know basis to the following recipients:

- staff members of the EPO and external users participating in or organising virtual events;
- staff members in the EPO's Productivity Apps, Collaboration & Events department and its third-party service providers for service maintenance and support purposes.

Personal data may be disclosed to Zoom and its third-party service providers for maintenance and support purposes. These are transfers to sub-processors outside of the EPO which are not covered by Article 8(1), (2) and (5) DPR. Your personal data will not be disclosed unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

5. How do we protect and safeguard your personal data?

We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access.

All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients.

For systems hosted on EPO premises, the following basic security measures generally apply:

- user authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege);
- logical security hardening of systems, equipment and the network;
- physical protection: EPO access controls, additional access controls to the data centre, policies on locking offices;
- transmission and input controls (e.g. audit logging, systems and network monitoring);
- security incident response: 24/7 monitoring for incidents, on-call security expert.

In principle, the EPO operates a paperless policy management system. However, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with a restricted access. When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out and the following general statement may be included in this field:

"For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. External providers are required to have implemented appropriate technical and organisational measures, such as physical security measures, access and storage control measures, securing data at rest (e.g. by means of encryption), user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging), and conveyance control measures (e.g. securing data in transit by means of encryption)."

Zoom has SOC 2 type II certification for compliance with security, availability, processing, integrity and confidentiality standards and its cloud services provider is ISO 27001 certified.

Zoom has publicly announced that it stores all data on third-party secured servers where the following security measures are implemented:

- management of access logs;
- 24/7 global support by managing and monitoring data centre access activities, equipping local teams and other support teams to respond to security incidents;
- backup power supply;
- data encryption.

For more information on the processing of personal data by Zoom (as independent controller) or its subcontractors, please consult its privacy policy. Zoom signs agreements with all its service providers that prevent them from processing of data for their own purposes or for the purposes of another third party.

When the EPO organises a virtual event on the Zoom platform and invites the parties to dial in, we will do so according to the most secure options available. The EPO nevertheless strongly recommends its users to only share any highly confidential data using Zoom's end-to-end encryption functionality (for more information, please refer to the User Technical Guidelines).

6. How can you access, rectify and receive your data, request that your data be erased or restrict/object to processing? Can your rights be restricted?

You have the right to access, rectify and receive your personal data, not to be subject to a decision based solely on automated processing, to have your data erased and to restrict and/or object to the processing of your data (Articles 18 to 24 DPR).

If you would like to exercise any of these rights, please write to the delegated data controller at DP_BIT@epo.org. In order to enable us to respond more promptly and precisely, you always need to provide certain preliminary information with your request. We therefore encourage you to fill in this form (for externals) or this form (for internals) and submit it with your request.

We will reply to your request without undue delay and in any event within one month of receipt of the request. However, Article 15(2) DPR provides that this period may be extended by two further months where necessary in view of the complexity and number of requests received. We will inform you of any such delay.

7. What is the legal basis for processing your data?

Personal data are processed on the basis of Article 5(a) DPR: "processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning … ".

For the legal basis for any recordings made during events, please refer to the privacy statement for the specific event.

8. How long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for they are processed.

Zoom retains the attendees' personal data that are strictly necessary for the organisation and management of a particular event/meeting for the maximum of one month.

Regarding Zoom recordings, the EPO's configuration allows only a restricted number of users to make recordings via Zoom and the necessity to record a particular event/meeting via Zoom is established by the relevant delegated controller at the EPO.

Zoom recordings are stored either locally on the user's computer or in the Zoom cloud (if the user is a licensed user). The locations and retention periods for Zoom recordings are decided by the EPO Delegated Controller that is accountable for the relevant event/meeting.

In the event of a formal appeal/litigation, all data kept on file when the formal appeal/litigation was initiated will be kept until the proceedings have been concluded.

9. Contact information

EPO staff who have questions about the processing of their personal data should contact the delegated data controller at DP_BIT@epo.org or the data protection officer at dpo@epo.org.

Externals may contact the delegated data controller and/or the data protection officer at DPOexternalusers@epo.org.

Review and legal redress

If you consider that the processing infringes your rights as a data subject, you have the right to request a review by the controller under Article 49 DPR and, if you disagree with the outcome of the review, the right to seek legal redress under Article 50 DPR.