Data protection statement on the processing of personal data in the context of Microsoft 365 applications

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.

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

This data protection statement relates to the processing of Microsoft 365 applications, which include the following cloud-based applications: OneDrive, SharePoint Online, MS Teams, MS Forms, Word, Excel and PowerPoint. The set of applications included in Microsoft 365 is provided to users with the aim of increasing flexibility and improving communication and collaboration, both within the EPO and between the EPO and external stakeholders.

As above-mentioned, Microsoft 365 applications include MS Teams, whose core features include business messaging, calling, audio and video meetings and file sharing. MS Teams is a cloud-based application to organise virtual meetings and teleconferences both within the EPO and between the EPO and EPO's stakeholders. In addition to these core features, MS Teams also allows the recording of virtual meetings and the use of live captions. The use of such features is granted to specific stakeholders only and in accordance with internal EPO policies on the use of MS Teams.

Furthermore, Microsoft 365 also includes non-optional 'connected experiences' which are designed to enable more effective creation, communication, and collaboration.

Microsoft 365 applications are used by EPO employees to fulfil their daily tasks.

In addition, personal data are processed for the following purposes established by the delegated controller, i.e. the EPO's Chief Information Officer (Business Information Technology (BIT) – Principal Directorate (PD) 4.6):

- Delivering Microsoft 365 applications and services to the EPO's staff and contractors.
- Providing end-user support and troubleshooting for Microsoft 365 applications and features.
- Managing content uploaded to Microsoft 365 applications.
- Managing Microsoft 365 settings.
- Supporting, operating, and maintaining the Microsoft 365 applications.

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

Microsoft Office 365 apps may be used for several different, specific purposes and scenarios, which the present data protection statement does not fully describe. The specific scenarios and purposes for which Microsoft 365 applications are used for processing personal data are described in dedicated data protection statements and associated records of processing activities.

Your personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR 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. In the context of usage of Microsoft's applications listed above transfers may occur for the following limited purposes: protection against malware, login to Azure Active Directory, load balancing, diagnostics data, connected experiences, and processing for Microsoft's business operations.

2. What personal data do we process?

In Microsoft 365 applications, the following categories and types of personal data may be processed.

In case the data subject is an EPO employee:

- Personal identification: first name, last name, picture, digital signature
- Contact information: work email address, phone numbers
- Employment information: company entity, department name and/or number, job title role, room number, office location, language preference (of communication)
- User Account information: user ID, account number, age of the account, ownership permissions, membership permissions
- Physical and/or digital identifiable assets: mobile device name, workstation hostname, operating system version
- Device Management data: last logon time, account ID
- Network/application interaction data: session metadata, session content, session details
- Geolocation information
- Browsing Information: browser type, browser user agent, website history, cookie information, URL, browsing date and time, IP address, network interaction history, browsing time
- Sensory and electronic information: presence status, audio information, visual information
- Telephony interaction data: telephony session metadata, telephony session content, telephony session details
- Phone call information: called phone number, caller phone number, phone call date and time, phone calling history, phone call interaction history, phone call duration
- System logs: file data (name, size and/or hash), registry data, running processes, port numbers, web server logs, system-/application-/ security-related server logs, audit logs, transaction-related details
- Personal information provided voluntarily by the data subject in the context of file sharing for professional activities (e.g. messages, images, files, voicemail, calendar meetings, contacts and the like) and any other additional information which the data subject might provide in the course of communication exchanges

In case the data subject is an external:

- Contact information: personal and/or working email address
- Network/application interaction data: session metadata, session content, session details
- Browsing Information: IP address, website history, browsing date and time, network interaction history, cookie information, URL, browser user agent, browser type
- Sensory and electronic information: presence status, audio information, visual information
- Telephony interaction data: telephony session metadata, telephony session content, telephony session details
- Phone call information: called phone number, caller phone number, phone call date and time, phone call duration, phone calling history, phone call interaction history.
- System logs: web server logs, system-/application-/ security-related server logs

- Personal information provided voluntarily by the data subject in the context of file sharing for professional activities (e.g. messages, images, files, voicemail, calendar meetings, contacts and the like) and any additional information which the data subject might provide in the course of communication exchanges.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the EPO's Chief Information Officer (BIT PD 4.6), acting as the EPO's delegated data controller.

Personal data are processed by PD 4.6 employees involved in managing the applications referred to in this statement.

External providers involved in supporting, operating and maintaining the Microsoft 365 applications – including but not limited to Microsoft itself - may also process personal data, which can include accessing it.

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:
• EPO staff and external users included in Microsoft 365 applications used for the exchange of information (for instance, the participants to an MS Teams meeting).
• EPO PD 4.6, Microsoft and PD 4.6 external provider's staff involved in the data processing necessary to provide the service.

In Microsoft 365 in principle the majority of the service operations are automated in order to reduce the need for human access. Any required access from Microsoft is for a limited time and with access rights limitations.

Where a virtual meeting is recorded in MS Teams, the recording may potentially be disclosed to the EPO as a whole, or outside the EPO, depending on the meeting. In either circumstance, the data subject will be duly informed by the meeting organiser of the details of the processing operation (e.g. by the means of a dedicated data protection statement).

For surveys/forms/questionnaires organised by an Owner via MS Forms, questions and answers are stored in Microsoft cloud. Access to a survey's submitted responses is available to the survey's owners only. In case of an anonymous survey, no contact information about the respondent is included in the response. In case of confidential surveys (= non anonymous), the owner has access to the respondent's name, email address, date and time when the respondent opened the survey, and data and time when the respondent submitted the response.

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

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

Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft 365 services is encrypted at rest. Regarding the implementation

of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft 365 Applications any required access by Microsoft is for a limited time.

Microsoft 365 applications implement and maintain multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft 365 services, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy.

Microsoft 365 applications have been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information you add to Microsoft 365, be it via chat, videoconference, or file sharing, will be available only to the specific users and groups indicated in section 4 above.

Microsoft 365 applications are certified under several security standards, including ISO27001, SOC1 Type II, SOC2 Type II, ISO27018 Code of Practice for Protecting Personal Data in the Cloud and complies with the requirements set forth in ISO27002.

Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

Personal data are stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented:
• In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors.
• Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft.

Specific measures relating to the recording of MS Teams meetings:

Where a virtual meeting is recorded, participants can limit the processing of their personal data by activating/de-activating their microphone and camera. In addition, where there are legitimate grounds, participants can also ask via the chat feature for the recording to be temporarily suspended so that they can contribute without being recorded.

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. External users should contact the DPO and/or the delegated data controller at DPOexternalusers@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 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'.

8. How long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which it is processed. More precisely personal data are kept as follows:

- Teams Chats, Teams Channel Messages, One Drive and SharePoint Online content are stored until EPO's termination of the contract with Microsoft.
- One Drive: personal data are automatically deleted from OneDrive one year after the user account has been deleted.
- MS Teams: if a Chat or Message in Teams is deleted by a user or if any content in OneDrive and SharePoint Online is deleted by a user, then it is retained for one year after the last modification date in an area only accessible by an administrator before a final deletion.

  For Teams, the history of phone calls is kept for 90 days and can be seen by administrators; an end-user can only see a 30-day-long own list of own phone calls.

  Recordings of Teams meetings made using the Recording feature are retained for a period of 3 months before deletion unless otherwise defined by the recorder. Recording of Live Teams events are kept for 180 days. Such recordings may be kept for longer than one year depending on the nature of the meeting, whereby the period of retention is defined in accordance with the purpose of the recording. If a recording becomes outdated or obsolete before the end of the retention period, it will be deleted. The specific retention period will be provided in a dedicated data protection statement and/or disclaimer which is sent with the invitation to the meeting.
- MS Forms: for surveys done via MS Forms the survey owner is responsible for defining, communicating and manually enforcing the retention they have decided.

In addition, at all times during the term of EPO's contract with Microsoft, EPO has the ability to access, extract and delete the data stored in the applications. Microsoft will retain EPO data that remains stored in the

applications in a limited function account for 90 days after expiration or termination of EPO's subscription so that EPO may extract the data. After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO data and personal data within an additional 90 days, unless Microsoft is authorized under the contract with EPO to retain such data.. For personal data in connection with the applications, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorised under the contract with EPO to retain such data.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at DP_BIT@epo.org for EPO staff members, or to DPOexternalusers@epo.org for external data subjects.
Internals may also contact our Data Protection Officer at dpo@epo.org, while externals may contact our 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 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.