Data protection statement on the processing of personal data by the EPO's Microsoft Defender for Endpoint service

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 security-relevant data by the EPO's Microsoft Defender for Endpoint (MDE) service. These data are collected from onboarded endpoints (Windows workstations and Windows servers) and transmitted to a segregated cloud tenant that is dedicated to the EPO's MDE service for processing and alerting in an automated manner. Business Information Technology (BIT)'s Principal Directorate (PD) 4.6 collects data related to MDE security alerts from the MDE cloud tenant and stores them on site in Splunk in an automated manner.

The EPO processes personal data to:

- prevent security incidents affecting the EPO's network and data, such as malware infections
- detect and flag compromising or malicious activity on endpoints in the EPO's infrastructure
- investigate and remediate security incidents in the EPO's infrastructure

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

Your personal data will not be transferred to recipients outside the EPO that 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.

2. What personal data do we process?

The following categories of personal data are processed.

In case the data subject is either an EPO employee or an EPO contractor (employee of an external service provider):

- personal identification: first name, last name
- contact information: phone numbers, working email address
- user account information: account number, user ID
- employment information: job title/role, department name and/or number
- network/application interaction data: session details, session metadata
- browsing information: time spent on browsing, browsing date and time, browser type, IP address, category, URL, website history, network interaction history
- device management data: Azure Active Directory device ID

- physical and/or digital identifiable assets: workstation network adapter MAC address, workstation serial number, operation system version, workstation host name (physical or virtual), vendor model of workstation, BIOS version, processor type, installed browsers extensions with indications of their state (active / inactive), installed certificates with indications of their properties, installed software applications
- system logs: audit logs (aka audit trails), system/application/security-related server logs, registry data, running processes, ports, file data (name, size and/or hash)

In case the data subject is an external user:

- Browsing information: time spent on browsing, IP address, network/application interaction data, session metadata

3. Who is responsible for processing the data?

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

Personal data are processed by the employees of Department 4.6.2.3 BIT Information Security involved in managing the service referred to in this statement.

External contractors involved in supporting and maintaining the Microsoft application – including Microsoft itself – may also access and process the personal data.

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

Personal data are disclosed via the MDE cloud tenant console on a need-to-know basis to the following recipients:

- EPO employees working in Department 4.6.2.3 BIT Information Security (only named individuals).
- Named individuals in PD 4.6 with the role of Microsoft O365 Global Administrator or Microsoft O365 Reader.

Personal data may be disclosed to third-party service providers acting on behalf of BIT for maintenance and support purposes. In principle, the majority of the service operations for Microsoft products are automated in order to reduce the need for human access. Any required access is for a limited time and subject to access rights limitations.

Personal data will only be shared with authorised persons responsible for the necessary processing operations and 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.

For personal data processed on systems not hosted on EPO premises, the EPO has carried out a privacy and security risk assessment. The providers that process the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks.

Any personal data transmitted over public networks between the EPO and Microsoft, or between Microsoft data centres, are encrypted by default. Personal data that are provided to Microsoft by, or on behalf of, the EPO through use of the Microsoft Defender for Endpoint service are 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 that are provided to

Microsoft by the EPO and role-based access controls to ensure that such personal data may only be accessed for legitimate service operations that are subject to management approval. As regards Microsoft services, any access required by Microsoft is for a limited time.

Microsoft implements and maintains multiple security measures for the protection of personal data that are provided to Microsoft by the EPO through use of the Microsoft Defender for Endpoint service. These security measures encompass the organisation of information security (e.g. security ownership, security roles and responsibilities, risk management programme), 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 maintains appropriate technical and organisational measures for the protection of any other personal data distinct from those described above. These measures are described in the Microsoft Security Policy.

Microsoft Defender for Endpoint has been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information collected through Microsoft Defender for Endpoint can be accessed only by the specific users and groups mentioned in section 4 above.

Microsoft Defender for Endpoint is certified in accordance with several security standards, including ISO27001, SOC1 Type II, SOC2 Type II and ISO27018 (Code of Practice for Protecting Personal Data in the Cloud), and complies with the requirements set forth in ISO 27002.

Microsoft conducts annual audits of the security of the computers, computing environment and physical data centres that it uses to process 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 subcontractors for processing in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of 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.

• For all transfers to third countries, Microsoft imposes EU Standard Contract Clauses for data transfer on its subcontractors for processing.

• Microsoft requires subcontractors for processing to join the Microsoft Supplier Security and Privacy Assurance Programme. 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.

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?

As a data subject, 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, i.e. where "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 processing necessary for the Office's management and functioning".

Personal data are processed on the basis of the following legal instrument: Article 7 "Monitoring, controls, audits and further processing" of Circular 382 (29 March 2017) EPO Information Security Guidelines.

8. For how long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which they are processed. More precisely, personal data are stored in accordance with the following retention rules.

- Data are kept in a temporary cache area in the endpoint itself for a maximum of three days.
- Data are kept in the MDE cloud environment for 180 days, after which they are deleted from the MDE cloud tenant.

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 (EPO employees) or DPOexternalusers@epo.org (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.