Data protection statement on the processing of personal data within the framework of Identity Management through Active Directory and Azure Active Directory.

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 provisioning of user accounts and related user access rules and allocations through the use of Active Directory (AD) and Azure AD as the central repository of user identities. The EPO uses Active Directory and Azure Active Directory for the purpose of Identity and Access Management.

Two scenarios for provisioning of user accounts are currently in place:

1. Internal (employees and contractors) users are defined in FIPS (master) which is synchronised with On Premise AD. Subsequently, the On Premise AD is synchronised with Azure AD.

2. Users of national patent offices: the master source is Single Access Portal, where users are created, updated and deleted, which is synchronised with On Premise AD. Subsequently, the On Premise AD is synchronised with Azure.

User accounts are thereafter used for authentication and authorisation purposes.

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 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.

2. What personal data do we process?

Processed personal data if the data subject is an EPO employee or a contractor:

- Personal identification data: first name, last name, gender, picture, preferred language of communication, digital signature, digital certificate
- Contact information: working email address, phone numbers, mobile phone number
- User account information: personnel number, user ID, account ID, account age, account password, password hash, last logon time, membership and ownership permissions
- Browsing information: browser type, browser user agent , browsing date and time, browsing time

- Network/application interaction data: session metadata, session details, IP address
- System logs: system-, application- and security-related server logs
- Device management data: Windows ID for Windows devices, tenant id, Azure Active Directory Device ID
- Employment information: department name and/or number, business unit division, personnel number, active/inactive indicator, line reporting manager, room number, job title role, office location, company entity (only for contractors).
- Physical and/or digital assets: workstation's hostname (physical or virtual), videoconference room/equipment identifier (only for Employees), mobile device name, operating system version.
- Building area and site

Processed personal data if the data subject is external:

- Personal identification data: first name, last name, country
- Contact information: working email address, phone numbers
- User account information: account number, account age, account password, password hash, membership and ownership permissions
- Browsing information: browser type, browsing time
- Network/application interaction data: session metadata, session details, IP address
- System logs: system-, application- and security-related server logs
- Employment information: company entity

Processed personal data if the data subject is a former employee:

- Personal identification data: first name, last name
- User account information: user ID, account age, account password, password hash, membership permissions
- Browsing information: browser type, browsing time
- Network/application interaction data: session metadata, session details, IP address
- System logs: system-, application- and security-related server logs

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 contractors involved in Identity and Access Management tasks may also process personal data, which can include accessing it.

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

The personal data are disclosed on a need-to-know basis to:

- EPO permanent and contractors staff (system administrators) of the Information Security Dept. 4.6.2.3.,
- All EPO staff: read access (directly via browser) e.g. via phone book or indirectly via APIs to other Microsoft applications (e.g. Outlook, MS Teams, etc.) to personal data of other EPO staff,
- AD/Azure AD personal data are accessed by EPO applications for user authentication/authorization purposes.

Personal data may be disclosed to third-party service providers for maintenance, support and security purposes.

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 Identity Management systems hosted at EPO premises, the following security measures are in place: All personal data related to Identity management are stored in secure IAM applications according to the security standards of EPO. These include:

- User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication;
- Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum;
- AV on all devices
- Physical protection: EPO access controls, additional access controls to datacentre,
- Transmission and input controls: audit logging, systems and network monitoring): security monitoring;
- Security incidence response: 24/7 monitoring for incidents, on-call security expert.

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. These systems 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 encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption)

Azure Active Directory is certified according to several security standards (e.g. SOC 1 Type II, SOC 2 Type II).

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, external users should write to the delegated data controller at DPOexternalusers@epo.org, while internals should write to 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), this form (for internals) and/or this form (for pensioners)) 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."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.

User data is kept until flagged inactive in the master (source) system (i.e. FIPS or Single Access Portal) and then kept in both On premise AD and Azure AD for additional 30 days.

At all times during the term of EPO's subscription, EPO has the ability to access, extract and delete the data stored in the applications in scope of this record. 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 agreement with EPO to retain such data.

For Personal Data in connection with the applications in scope of this record, 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 authorized under the agreement 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

External data subjects who have any questions about the processing of their personal data should contact the Data Protection Officer and/or the delegated data controller at DPOexternalusers@epo.org.

EPO Employees should contact the delegated data controller at DP_BIT@epo.org, and the Data Protection Officer at dpo@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.