Data protection statement on the processing of personal data in the context of the meetings of the Administrative Council and its bodies

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 Data Protection Rules of the Administrative Council (AC DPR).

The information in this statement is provided in accordance with Article 6 AC DPR in conjunction with Articles 16 and 17 of the Data Protection Rules of the European Patent Office (DPR).

This data protection statement explains the way in which personal data are processed for the management and the conduct of the meetings of the Administrative Council and its bodies being held as e-meeting, on-site or in hybrid mode.

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

This data protection statement explains the way in which personal data are processed in relation to the meetings of the Administrative Council and its bodies.

Your personal data are collected and processed by the Council Secretariat in order to ensure the smooth organisation, administration and running of such events, via the videoconferencing platform Zoom, the voting platform Linkando, document managements tools such as OpenText, Sharepoint or OneDrive.

In addition, your personal data re processed for compiling official records e.g. record of chat messages, invitation, participation, voting and distribution of relevant documents, as applicable, also using the audio recording functions in Zoom, the transcription tool Sonix, and then Microsoft Copilot, an AI based productivity tool. The meeting’s official records (minutes) are also published on the MICADO Documents database.

Furthermore, in case of physical attendance, personal data are processed by the Physical Security| Facility Management Munich in order to maintain an up-to-date badge system. Additionally, personal data of the onsite participants entitled to reimbursement are processed via an online reimbursement tool in Single Access Portal (SAP).

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 7 AC 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 Council Secretariat processes the following categories of personal data:

- country
- preferred language
- first and last name
- business address
- title
- department and name of the employer National Patent Office (NPO) when applicable
- phone number
- mobile number (optional)
- email address
- the role held in a body of the Council (e.g., representative, alternate, external expert participating in Council meetings) and start and end date in such role (both when applicable)
- signature
- travel booking details (if applicable)
- bank account number and bank details
- dietary preferences and restrictions (if applicable)

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Head of the Council Secretariat, acting as the AC delegated data controller.

Personal data are processed by the Council Secretariat staff involved in managing the initiative, project and activity referred to in this statement.

External contractors involved in providing platforms for virtual meetings as well as services for the organisation and safety of meetings 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 EPO staff working in the Council Secretariat, D412 Treasury & Accounting, D4615 Productivity and Collaboration CoE, D444 Language Services, and D442 Building Management Munich/Vienna.

Personal data may be disclosed to third-party service providers for badge production, security services, storage purposes and to the providers of voting and videoconference platforms.

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 network
- Physical protection: EPO access controls, additional access controls to datacentre, 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.

The EPO has adopted 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.

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).

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 6 AC DPR).

If you would like to exercise any of these rights, please write to the delegated data controller at DPCouncil@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), form (for internals) or 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?

Processing is conducted in accordance with Article 4(a) AC DPR as it is it is necessary for the performance of a task concerning the Administrative Council's exercise of its official functions or any other activity mandated under the European Patent Convention. In case special categories of personal data (i.e. dietary restrictions) are processed, the applicable legal bases are Article 4(a) AC DPR in conjunction with Article 5 AC DPR and Articles 11(2) and 12 DPR.

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.

As a general rule, they are retained as long as obligations by the Council exist including adequate time to check the fulfilment of those obligations for a maximum of 3 years.

A minimum of selected personal data is kept indefinitely**,** if justified for, inter alia:

- historical purposes in the public interest (see Minutes under Article 12(2) AC Rules of Procedure
- historical institutional purposes (e.g., portraits and pictures taken of Council chairpersons)

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 DPcouncil@epo.org.You can also contact our Data Protection Officer at dpo@epo.org.

External users are encouraged to contact us or our Data Protection Officer via the following email address: 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 11(1) AC DPR and, if you disagree with the outcome of the review, the right to seek legal redress under Article 12(1) AC DPR.