

## **Data protection statement<sup>1</sup> on the processing of personal data in the organisation of meetings of the Standing Advisory Committee before the EPO (SACEPO)**

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.

A dedicated advisory body, the Standing Advisory Committee before the European Patent Office (SACEPO) brings together a wide range of user representatives (patent attorneys and industry representatives) to advise and provide input on proposals and projects to develop the European patent system and on the EPO's activities. Meetings are organised for both the Main SACEPO and its five specialised committees or Working Parties (Quality, Rules, Guidelines, Patent Information and Documentation, e-Patent Process). This data protection statement relates to the personal data that are processed during the organisation of these meetings.

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

Personal data of the participants in the meetings are already obtained during the SACEPO membership selection process and are used by the delegated controller to organise these meetings. The meetings are chaired by the President of the EPO and other EPO representatives. There are also EPO staff present at the meetings, and exceptionally external experts. The organisation of the meeting and any sharing of documents and minutes is conducted through the generic email address for SACEPO ([sacepo@epo.org](mailto:sacepo@epo.org)).

Where meetings occur virtually, Microsoft Teams is used. When the meetings occur in person, dietary requirements may be collected, and financial details may be collected to provide reimbursement where any costs are to be borne by the EPO.

Personal data are processed to plan, organise and run the SACEPO meetings. This includes:

- the organisation and actual conducting of the meetings
- the distribution of documents, agendas and minutes
- in case of physical meetings, the data necessary for reimbursement of costs and any dietary requirements
- in case of virtual meetings, the provision of technical support as necessary
- the preparation for the meetings by the EPO's representatives
- to keep track of the consultation process for future reference and archiving

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

---

<sup>1</sup> Version June 2022

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:

- identification and contact details (mainly name, email address, phone number, nationality, organisation/company and field of technology for external participants, position in the EPO for internal participants)
- role in the process (e.g. SACEPO member, external expert, EPO participant)
- information related to the meeting
  - o specialist SACEPO working group in which the person is involved
  - o agenda, minutes, list of participants
  - o any information, written and oral contributions, documents shared with SACEPO
  - o personal data included in exchanges
  - o in case of physical meeting, possibly dietary requirements
  - o financial details where necessary for reimbursements

## **3. Who is responsible for processing the data?**

Personal data are processed under the responsibility of PD52 Legal Affairs acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in organising the SACEPO meetings including D 5.2.2 European and International Legal Affairs, PCT, PD41 Finance (where reimbursements for costs are necessary) and PD46 BIT/CIO (where the technical support for virtual meetings is required). Personal data may also be shared with EPO senior management and other EPO staff that are participating in the meetings.

External contractors involved in providing a platform for virtual meetings or services necessary for the organisation of meetings may also process personal data, which can include accessing it. This includes Microsoft, Thomson Reuters, SAP and OpenText.

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

EPO staff from D 5.2.2 European and International Legal Affairs, PCT have access to the personal data described above.

Personal data are disclosed on a need-to-know basis to the EPO staff working in PD41 Finance (where reimbursements for costs are necessary) and PD46 CIO/BIT (where technical support for virtual meetings is necessary).

Personal data may also be disclosed to the participants of the meetings (in the list of participants, agenda and minutes). These personal data may also be shared with the business associations which are asked by the EPO to nominate representatives as SACEPO members.

Personal data will be shared outside of the EPO on a need-to-know basis including to external participants in the meetings and to the business associations whose delegates are SACEPO members.

Personal data may be disclosed to third-party service providers for the provision of services necessary for the organisation of the meetings and the provision of virtual meeting 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.

Data Processing Agreements have been concluded with the external contractors involved in providing the services necessary for organising the meetings and providing a virtual platform.

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.

In principle, 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 18 to 24 DPR).

The right to rectification can only apply to inaccurate or incomplete factual data processed in the context of the EPO's tasks, duties and activities; it does not apply to subjective statements, including ones made by third parties.

If you would like to exercise any of these rights, please write to the delegated data controller at [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org) for external data subjects. EPO employee data subjects should contact [pdlegalaffairs-dpl@epo.org](mailto:pdlegalaffairs-dpl@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 DPR:

- (a) 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.

The following retention periods apply:

- where dietary requirements are collected, this data is deleted three months after the event
- should invoices be sent to the delegated controller, these invoices are deleted after three years
- other personal data of SACEPO members processed in relation to meeting of SACEPO and user consultations is kept for three years after the end of their SACEPO membership

The minutes of SACEPO meetings are anonymised and are thereafter kept without limitation of time.

Possible archiving activities are addressed in a separate data protection statement.

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, external data subjects can write to the delegated data controller at [dpoexternalusers@epo.org](mailto:dpoexternalusers@epo.org), and EPO employees can write to [pdlegalaffairs-dpl@epo.org](mailto:pdlegalaffairs-dpl@epo.org).

Internals may also contact our Data Protection Officer at [dpo@epo.org](mailto:dpo@epo.org), while externals may contact our Data Protection Officer at [DPOexternalusers@epo.org](mailto: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.