

## Data Protection Statement<sup>1</sup> on the processing of personal data in the context of the Convergence of Practice programme

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to respecting and protecting your personal data and ensuring your rights as a data subject. All data of a personal nature that identifies you directly or indirectly will be processed lawfully, fairly and with due care.

This processing operation is subject to the EPO Data Protection Rules ([DPR](#)). The information in this communication is provided pursuant to Articles 16 and 17 of the DPR.

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

The purpose of this processing by Principal Directorate 5.2 Legal Affairs (PD 5.2) is the implementation of the Office's international co-operation programme on the convergence of practice. This implementation requires the identification of the individuals representing the States or associations which participate in the discussions organised by the EPO, the setting up of corresponding lists, organisation and holding of meetings, the sharing of opinions on the document to be prepared etc.

Personal data are processed for the following purposes:

- Identify participants
- Facilitate the necessary exchanges of views between the stakeholders involved
- Elaborate a common proposal to be adopted by the Administrative Council of the EPO
- Keep track of the elaboration process, for historical and legal certainty purposes

### 2. What personal data do we process?

The delegated controller collects and otherwise processes identification data (e.g. name, State or association represented), contact data (e.g. email address), and any other personal data which may otherwise be provided by the participants regarding themselves or other individuals in the context of the consultation such as description of concerns, opinions.

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

The processing of personal data is carried out under the responsibility of the Principal Director Legal Affairs (PD 5.2), acting as the EPO's delegated data controller.

### 4. Who has access to your personal data and to whom is it disclosed?

The staff of Directorate D 5.2.2 (European and International Legal Affairs, PCT) involved in this project will have access to the data.

The personal data might be disclosed on a need-to-know basis (e.g. list of participants) to the participants of the working group, senior management of the EPO or other units.

Personal data is disclosed to third-party service providers for maintenance and support purposes. Those service providers are Microsoft, OpenText, TRE Thomson Reuters and Zoom.

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

---

<sup>1</sup> Version February 2023.

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

All personal data are stored in secure IT applications according to the EPO's security standards. Appropriate levels of access are granted individually only to the abovementioned recipients.

For systems hosted at EPO premises, the following base 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 to lock offices
- Transmission and input controls (e.g. audit logging, systems and network monitoring)
- Security incidence response: 24/7 monitoring for incidents, on-call security expert.

For personal data processed on systems not hosted at EPO premises, the provider(s) processing the personal data has committed in a binding agreement to comply with its data protection obligations stemming from the applicable data protection legal framework(s). Furthermore, a privacy and security risk assessment has been carried out by the EPO. 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).

If you would like to exercise any of these rights, please write with details of your request to the delegated data controller at [legalaffairs-dpl@epo.org](mailto:legalaffairs-dpl@epo.org). If you are an external user, you can contact the DPO directly at [dpoexternalusers@epo.org](mailto:dpoexternalusers@epo.org).

We will reply to your request without undue delay, and in any event within one month of receipt of the request. However, according to Article 15(2) of the DPR, that period may be extended by two further months if necessary, taking into account 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 is processed in accordance with Article 5a DPR: Processing is necessary for the performance of a task carried out on the basis of legal provisions of the European Patent Organisation or in the legitimate exercise of the official authority vested in the EPO, and in particular to execute the tasks of the Strategic Plan adopted by the Administrative Council of the EPO.

## **8. How long can data be kept?**

There is no personal data included in the Minutes and Reports.

Personal data processed in email correspondence as well as the list of participants may be stored for the default retention period of the delegated controller, which is 20 years.

This retention period applies without prejudice to possible archiving (archiving activities are addressed in a separate statement).

## **9. Contact information**

If you have any questions about the processing of your personal data, please write to the delegated data controller at [legalaffairs-dpl@epo.org](mailto:legalaffairs-dpl@epo.org). You can also contact our Data Protection Officer at [dpo@epo.org](mailto:dpo@epo.org).

If you are an external data subject, you can contact the 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 data subject, you have the right to request review by the controller under Article 49 DPR and the right to seek legal redress under Article 50 DPR.