

## **Data protection statement on the processing of personal data in the context of EPO's outreach activities**

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.

This data protection statement refers to the outreach activities carried out by the Customer Journey directorate. Customer Journey helps users get the best customer experience in their interaction with the EPO by

- reaching out proactively
- providing Key Account Management services
- solving enquiries
- supporting Customer Engagement
- monitoring the Customer Enquiries resolution
- coordinating User Satisfaction surveys
- administering complaints
- monitoring Customer Intelligence data coming from user interactions

The Customer Journey directorate focuses on business intelligence, contacts and relations with key users, promoting new services and tools, offering online services training and user days as well as tailor-made workshops and market research. It also organises workshops and conferences in cooperation with units across the EPO. The latest customer outreach activities include meetings with key users from industry. Dedicated meetings with SMEs and private applicants are offered as well to meet the specific needs of this user segment.

The data processed by Customer Journey derives partly from the Customer Services Management (CSM) tool as defined in the corresponding data protection statement on <https://www.epo.org/en/about-us/office/data-protection-and-privacy> under "Information on the processing of personal data in EPO products and services" under "For the management of interactions with users contacting the EPO", item 8. Additional data can also be drawn from the BIT and DG4 Corporate Services databases regarding the use of EPO online services.

This data protection statement focuses on the outreach activities where staff from the Customer Journey directorate contact customers in a proactive way.

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

This data protection statement explains what personal data are processed for the purpose of executing EPO's outreach activities, and how. These activities include

1. promoting large scale events aimed at informing users of the latest developments at the EPO, such as the EPO User Day, by contacting EPO users (data subjects),

2. promoting events related to EPO Online Services to inform users of the latest developments, how to best use the EPO Online Services, collect feedback and reply to questions, by contacting EPO users (data subjects),
3. promoting workshops on specific relevant topics such as the latest developments of EPO tools or services or legal changes, targeted to specific users by contacting these specific users (data subjects),
4. contacting users to solicit feedback on EPO Online Services,
5. informing users on relevant information related to the EPO Online Services,
6. informing users on relevant information related to the EPO's user outreach activities.

Persons who can be contacted include:

1. individuals who have contacted the EPO for enquiries, have their contact details stored in the EPO customer database and have not objected to receiving further communications from the EPO,
2. individuals who have registered for a previous EPO event and who have not objected to receiving further communications from the EPO,
3. Users (i.e. companies, applicants or patent attorney firms) of the following services:
  - MyEPO Portfolio services
  - Online Filing 2.0 service
  - 'Legacy' online services such as eOLF
  - EPO smart card

To achieve this purpose, the EPO sends an e-mail to the users providing the relevant information via an external mailing tool or via an e-mail from an EPO employee.

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?**

The following categories of personal data are processed:

- E-mail address.
- Full name and address
- MyEPO Portfolio account ID
- Company name

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

Personal data are processed under the responsibility of the Customer Journey and Key Account Management principle directorate, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the initiative, project or activity of the Key Account Management and Customer Services departments referred to in this statement.

The EPO's BIT Corporate Services department, which might include external contractors involved in promoting the event or retrieving the use of EPO Online Services mentioned under paragraph 1 above, 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 Customer Journey directorate.

Personal data may be disclosed to third-party service providers for support 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 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.

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).

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). 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](#) and submit it with your request.

We will reply to your request without undue delay and in any event within one month of receiving 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 based on Article 5(a) DPR: '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.

Personal data processed for this purpose will be deleted five years after the date of collection.

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 [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org).

You can also contact our Data Protection Officer at [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org).

## **10. Review and legal redress**

If you believe that the processing infringes your rights as a data subject, you have the right to request a 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.