Data protection statement on the processing of personal data for post-grant contact management

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.

Personal data are processed for the purpose of communicating with contacts from National Patent Offices in contracting member states with respect to monitoring Article 39 EPC.

When communicating about patents, only patent numbers or application numbers are used to identify patents.

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

This data protection statement relates to the processing of post-grant contact management.

A list of contact persons at National Patent Offices is maintained for the purpose of administering post-grant validation activities and communicating with respect to monitoring Article 39 EPC. The National Patent Office contact persons provide the EPO with their contact details.

The contact list is stored on EPO internal storage systems and communication is carried out using MS Outlook via the shared mailbox PostGrant@epo.org.

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?

The following categories of personal data are processed:

From employees: contact details, phone number, working email address, job title role, first name, surname, full name.

From externals: contact details, phone number, working email address, job title role, first name, surname, full name.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of PD41/D412 Revenue Controls, PD41 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 D412 Revenue Controls referred to in this statement.

External contractors involved in maintaining communication services may also process personal data, which can include accessing it. Microsoft is the external provider of IT applications.

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 International Cooperation, member states and neighbouring countries, Legal Services and Finance.

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

Personal data will only be shared with authorised persons responsible for necessary processing operations. It 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.

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.

When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out and the following general statement might be included in this field:

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 PDFinanceDPL@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 external data subjects) 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 (a) and (b) DPR which read as follows:

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, or
b. processing is necessary for compliance with a legal obligation to which the controller is subject

Personal data are processed on the basis of Art. 39 EPC.

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.

Contact details are kept in the respective function at a National Office. They may be deleted if it can reasonably be expected that there is no longer any operational need to retain them. Personal data will be erased at the very latest three years after somebody has left their function at a National Office.

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 PDFinance-DPL@epo.org.

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