Data protection statement[1] on the processing of personal data in the context of the maintenance of lists of associations

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.

The Legal Division of the EPO within Directorate 5.3.2 Procedural Guidance and Registers is responsible for the registration and deletion of associations.

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

Pursuant to Article 134(1) EPC, representation of natural and legal persons in proceedings established by the EPC may only be undertaken by professional representatives whose names appear on a list of the EPO maintained for this purpose. Pursuant to Rule 152(11) EPC, an authorisation of an association of representatives shall be deemed to be an authorisation of any representative who can provide evidence that they practise within that association. This legal fiction allows a party to authorise several representatives as an association instead of singly, provided this association is registered with the EPO.

This data protection statement explains the way in which the personal data are processed for the sake of registration, changes or deletions of associations.

Personal data are processed for the following purposes:

- registration, administration and deletions of associations by the EPO
- providing up-to-date information to competent units in the patent grant process to ensure a proper and efficient information flow and management of associated activities
- registration, administration and deletion of associations and associated respective entries in the European Patent Register
- preparation of statistics

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 (or might be) processed:

- identification and contact information (such as name, signature, professional email address)
- information related to representation in the patent granting process (such as representative ID number,

[1] Version November 2024

affiliation to association, supporting documentation provided), including, as the case may be, information on professional memberships
- correspondence, including documents provided
- ticket-related data
- name and contact details of the EPO employee dealing with the matter (such as job title, department)

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Principal Directorate 5.3 Patent Law and Procedures, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in the activity of PD 5.3 referred to in this statement.

External contractors (Microsoft and ServiceNow) involved in providing certain services may also process personal data, which can include accessing these data.

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

Personal data are accessed by the EPO staff working in Principal Directorate 5.3 Patent Law and

Proceduresby the legal division within Directorate 5.3.2 Procedural Guidance and Registers. Other business

units at the EPO will have access to the information stored on the contact details database:
- DG0, DG1, DG5
- with other involvements also being possible, e.g. the Board of Appeals on a need-to-know basis

Personal data may be disclosed to the aforementioned third-party service providers for maintenance and 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 the 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 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 EPO has carried out a privacy and security risk assessment. The providers processing the personal data have committed in a binding agreement to complying 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 means of encryption)
- user, transmission and input control measures (e.g. network firewalls, a network intrusion detection system (IDS), a network intrusion protection system (IPS), audit logging)
- conveyance control measures (e.g. securing data in transit by means of 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 those made by third parties. The right to erasure does not apply if the legal obligation on the controller (e.g. to maintain the list of associations) requires the processing of personal data.

To exercise any of these rights, external users should write to DPOexternalusers@epo.org; otherwise, contact the delegated data controller at pdpatentlaw-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(a) DPR: the 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 EPO's management and functioning.

Personal data are processed on the basis of the following legal instruments: Art. 20 EPC, Art. 134 EPC, Art. 134a(2) EPC, Rule 143(1)h EPC, Rule 152(11) EPC, Rule 154 EPC and the Decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division, OJ EPO 2013, 600.

8. How long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which they are processed.

For reasons of legal certainty, personal data are kept for up to 99 years, starting from the deletion date of the association.

Personal data of professional representatives will be deleted after 99 years from the first date of entry of the professional representatives to cover the average lifetime of a professional representative and any related post-procedural and disciplinary consequences arising therefrom (also related to association membership).

9. Contact information

If they have any questions about the processing of their personal data, externals should contact the DPO and/or the delegated data controller at DPOexternalusers@epo.org. EPO employees should contact the delegated data controller at pdpatentlaw-dpl@epo.org or the Data Protection Officer at dpo@epo.org.

Review and legal redress

If you believe 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.