

## **Data protection statement<sup>1</sup> on the processing of personal data in the context of the administration of the Register for Unitary Patent Protection**

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 Unitary Patent Protection Division is responsible for maintaining the Register for unitary patent protection (UP Register). The Unitary Patent Protection Division is part of the Principal Directorate 5.3 Patent Law and Procedures. This data protection statement relates to the processing of personal data for the purposes of the administration of the UP Register.

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

Rule 15 UPR refers to the establishment of the UP Register. The UP Register provided for in Article 9, paragraph 1(b), Regulation (EU) No 1257/2012 is established as a special part of the European Patent Register kept by the EPO under Article 127 EPC.

Personal data is received:

- internally via electronic means, or in exceptional cases, by post,
- when the procedural step is in scope of the Unitary Patent Protection Division, or
- when guidance or legal advice is sought from the Unitary Patent Protection Division.

A member of the Unitary Patent Protection Division assesses the facts and takes a decision on whether a change must be made in the register. In rare cases, the matter may require legal advice (see the corresponding record on legal advice related to institutional issues and activities of the Legal Division and Unitary Patent Protection Division). This decision is registered electronically, after which the Register is updated automatically. A communication is then sent to the relevant party. If the representative is a user of electronic tools, the communication is automatically sent there, otherwise per post.

In case a request reaches the Unitary Patent Protection Division, the ticketing system sends automatic emails to the mailbox of the Unitary Patent Protection Division. These emails do not contain any personal data, they only provide a ticket number and a link to access the ticketing system. The requester receives their answer via this ticketing system.

In exceptional cases where the requesters have further questions, they can contact the Unitary Patent Protection Division directly via email. In such cases, corresponding personal data is shared via email.

All documents filed in proceedings before the Unitary Patent Protection Division are stored.

---

<sup>1</sup> Version January 2026

The data subjects concerned are proprietors, representatives, opponents and third parties.

The processing activities described above are required to enable the Unitary Patent Protection Division to administer the UP Register. This processing of your data 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?**

With regards to external data subjects, the following categories of personal data may be processed:

- personal identifying data, including contact details (e.g. name, email address, phone number, passport or national identity card number);
- employment information (company entity, job title);
- information related to the UP Register (address, any personal data included in the patent);
- other data (any personal data provided in the course of correspondence (e.g. evidence provided pursuant to Rule 20(2) UPR in conjunction with Rule 22 EPC), ticketing data, in rare cases health-related data (e.g. evidence provided pursuant to Rule 20(2) UPR in conjunction with Rule 142(1)(a) EPC related to an interruption of proceedings due to legal incapacity), and financial data in the event that a refund is issued by the Office).

With regard to EPO staff in their capacity as data subjects, the following categories of personal data may be processed:

- personal identifying data, including contact details (name, phone number);
- employment information (business unit, job title)

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

Personal data is processed under the responsibility of PD 5.3 Patent Law and Procedures. Personal data is processed by the EPO staff in the Unitary Patent Protection Division, part of PD 5.3 Patent Law and Procedures, who are maintaining the UP Register.

Personal data is also processed by EPO staff in D 5.4 Patent Intelligence, and EPO staff in DG 1 Patent Granting Process.

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

Personal data is accessed by EPO staff working in the Unitary Patent Protection Division. Personal data may be disclosed on a need-to-know basis to EPO staff working in PD 5.4 Patent Intelligence and in DG 1 Patent Granting Process. Personal data may be disclosed to EPO staff with Madras access. Personal data may also be disclosed to trustees outside of member states who are notified about the information to be published in the UP Register.

All personal data recorded in the UP Register are accessible to the public.

Personal data may be disclosed to third-party service providers, such as Microsoft and ServiceNow, for the purposes of the provision and maintenance of tools and services necessary for the administration of the UP Register.

Personal data will only be shared with authorised persons responsible for the necessary processing operations and 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 is 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

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), unless the EPC, the PCT or any practices or provisions applicable under them require differently in relation to personal data processed in the patent granting and related procedures (see the Decision of the President of 13 December 2021, OJ EPO 2021, A98).

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 where the legal obligation on the controller requires the processing of personal data. With regards to the right of access, if the EPO considers it necessary to protect the confidentiality of internal deliberations and decision-making, certain information may be deleted from the copy of personal data provided to the data subject.

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 users and [pdpatentlaw-dpl@epo.org](mailto:pdpatentlaw-dpl@epo.org) for EPO employees. 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 is processed on the basis of Article 5 DPR (a) and (b):

- where 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, and
- where processing is necessary for compliance with legal obligation to which the controller is subject.

Personal data is processed on the basis of Rule 20(2) UPR in conjunction with Rules 22, 23, 24, 142 EPC, and the decision of the President of the European Patent Office dated 30 May 2022 concerning the allocation of the tasks to be carried out by the European Patent Office in relation to the European patent with unitary effect and concerning the entrustment of duties incumbent on the Unitary Patent Protection Division (OJ EPO 2022/A69).

## **8. How long do we keep your data?**

For reasons of legal certainty, personal data processed in the context of the administration of the UP Register is kept for an indefinite period.

Personal data for non-patent-file-related matters are kept for the default retention period for legal and procedural advice for legal affairs (20 years). Rare cases in which high-ranked officers of the EPO (e.g. President of the EPO or Vice-President DG5 International and Legal Affairs) were involved in order to be able to document the decision-making process are an exception.

In the event of a formal appeal or litigation, all data kept on file when the formal appeal/litigation was initiated will be kept until the proceedings have concluded.

## **9. Contact information**

If any questions about the processing of their personal data arises, external data subjects can write to the delegated data controller at [dpoexternalusers@epo.org](mailto:dpoexternalusers@epo.org), and EPO employees can write to [pdpatentlaw-dpl@epo.org](mailto:pdpatentlaw-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.