

## **Data protection statement on the processing of personal data in the context of off-site storage of patent granting process (PGP) paper files**

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.

Paper originals submitted by users of the EPO's patent grant process are scanned and kept on-site for a number of months in case scanning problems are detected.

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

This data protection statement explains the way in which the personal data available in the paper files are processed.

After scanning, the original paper is stored in boxes. After the initial on-site storage period, the boxes are transported either from The Hague or Munich to the off-site storage contractor in Amersfoort, Netherlands, where they are stored in a secure warehouse. At the EPO's request (a rare occurrence that happens about 10 times per year), a document may be retrieved from a box and sent back to the EPO either in the original paper format or as a scanned electronic version. In line with legal retention periods, the EPO initiates safe destruction of the boxes. They are retrieved from the storage warehouse and transported to a specialised destruction company, which carries out the secure destruction.

In relation to the digital processing of the files, reference is made to the data protection statements (DPS) relating to the:

- Processing of personal data in the context of EPO smart cards
- "MyEPO Portfolio" online service for parties to proceedings before the EPO (PGP)
- "EPO Contingency Upload Service" for parties to proceedings before the EPO (PGP)

Personal data are processed in line with the legal requirements under Rule 147 of the Implementing Regulations to the Convention on the Grant of European Patents and section 705*bis* PCT.

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:

- **In relation to EPO employees and persons involved in the patent granting process i.e. applicants/proprietors, representatives, inventors and opponents:**
  - Business unit division (if applicable)
  - First name
  - Surname
  - Full name
  - Telephone numbers
  
- **Bibliographic data used in the patent granting process:**
  - Name
  - Address
  - City
  - Country
  - Telephone number
  - Email address
  
- Authors of publicly available prior art may also be included.
- The EPO user IDs of contract staff who have indexed a document on paper data sheets are printed for each batch to be scanned.

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

Personal data are processed under the responsibility of Directorate-General 1's Chief Operating Officer (Principal Director 1.1), acting as the EPO's delegated data controller.

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

The external contractor involved 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 Directorate 1.1.9.5 "Classification Support, File Management, SCAPEs and CDR" in interaction with the external contractor.

Personal data may be disclosed to 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 to the above-mentioned recipients only.

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.

Paper files containing personal data stored on EPO premises are locked in a secure location with restricted access.

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. 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). The paper file boxes are stored in a secure warehouse and the external contractor has signed a contract, which includes clauses on technical conditions, security details and a confidentiality agreement.

## **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).

As with all secondary legislation adopted by the Administrative Council in accordance with its powers under Article 33(2) EPC, the DPR are subject to the provisions of the EPC, including its Implementing Regulations, which form an integral part of the EPC under Article 164(1) EPC. In addition, where the EPO is acting as PCT receiving Office and International Authority, it is bound first by the PCT legal framework, which consists of the Patent Cooperation Treaty, its Regulations and the related secondary law, i.e. the Administrative Instructions, the Guidelines for receiving Offices and the International Searching and Preliminary Examination Guidelines. Accordingly, any data subject rights under the DPR apply only to the extent that they do not conflict with the provisions of the EPC and its Implementing Regulations and, where applicable, of the PCT legal framework.

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 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 5a DPR (processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation).

Personal data are processed on the basis of the legal requirements in Rule 147 of the Implementing Regulations to the Convention on the Grant of European Patents and section 705bis PCT.

In particular, personal data are processed for the purposes of the EPO's task under Article 4(3) EPC of granting European patents, as further specified in the relevant provisions of the EPC and the other provisions applicable under it. Where these data are required for proceedings under the EPC, their processing is mandatory (mandatory personal data). The same applies *mutatis mutandis* to data required for proceedings under the PCT.

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

It is a legal requirement to keep the original paper submissions for five years from the end of the year they were filed in. Leaving a safety margin of one year, the EPO destroys scanned original papers that are older than six years old. In other words, personal data contained in paper files is deleted after six years.

However, any paper files earmarked for use for artistic and historical purposes will be kept in the EPO's cultural space for no longer than 60 years from the end of the year they were filed in.

## **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).

## **10. 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.