

## **Data protection statement on the processing of personal data within the framework of the delivery of Patent Information Services for Experts (PISE).**

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.

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

This data protection statement relates to the processing of personal data in the context of the Patent Information Services for Experts (PISE)

The European Patent Office (EPO) provides web based Patent Information Services for Experts (PISE) to users. Prior to dissemination, the data is processed into the form ready to be disseminated.

Some PISE services require user registration which is linked to an integrated Internet Access Control based upon user credentials.

The patent procedure records may also contain personal information as an intrinsic part of the subject matter treated in the record (inventors, applicants, EPO officers etc).

In addition to the above mentioned "content" processing, additional processing is undertaken in order to provide service usage analytics and ensure correct service functioning.

The purpose of the processing operations is to deliver the PISE services to users and undertake analytics relating to the service delivery.

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 for EPO employees and externals (not all the categories are processed for every data subject):

The following categories of personal data are processed:

- Patent Process Related Data: Patent Record Bibliographic and Meta Data, Personal data potentially included within the content of patent procedure related information and publications
- Browsing Information: Browser type, Browsing Time, Cookie Information, IP Address, Network Interaction History, Website History
- Contact Information: Contact Details, Country, Personal Email, Working email address
- Employment Information: Company Entity
- Network/application Interaction Data: Session content, Session details, Session metadata
- Personal Identification: First Name, Full Name, Gender, Surname
- User Account Information: Account Password, User ID.

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

Personal data are processed under the responsibility of the Principal Director of the Patent Intelligence Principal Directorate acting as delegated EPO data controller.

Personal data are processed by the EPO staff involved in providing and maintaining the services referred to in this statement.

External contractors involved in providing and maintaining certain services may also process personal data, which can include accessing it.

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

The patent record content can be made available to anyone who uses the service. These users may be located world-wide.

Personal data of users may be shared with authorised persons responsible for the corresponding processing operations, including EPO staff and external contractors, and any other EPO staff members who need to have access to the data only on a need to know basis.

### **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.

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).

## **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?**

As a data subject, 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, external users should write to [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org), otherwise contact the delegated data controller at [PDPatentIntelligence-DPL@epo.org](mailto:PDPatentIntelligence-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 is processed on the basis of Article 5(a) of the DPR, i.e. 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?**

User data are retained for up to 7 years or deleted earlier once it can be reasonably expected that there is no immediate operational need anymore

Technical service access data can be retained for up to 7 years in order to analyse usage patterns.

The personal data in the patent records is public data which is never deleted.

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**

External data subjects who have any questions about the processing of their personal data should contact the Data Protection Officer and/or the delegated data controller at [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org).

EPO employees should contact the delegated data controller at [PDPatentIntelligence-DPL@epo.org](mailto:PDPatentIntelligence-DPL@epo.org).

Internals may also contact the 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.