

Data protection statement on the processing of personal data within the framework of the Patent Knowledge Web Shop

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 Knowledge Web Shop.

The EPO online shop is an web based platform where individuals can order EPO Patent Knowledge related products and services where Patent Knowledge is understood to be knowledge that serves to foster the effective use and dissemination of patent data.

Personal data are processed and used as described below:

- Personal data is collected and processed for the purpose of processing orders and promotion and marketing activities of the EPO.
- The personal data of EPO online shop customers is collected during user account registration process. Customers connect to the EPO online shop area of the EPO website to register and/or maintain their account information. An account is required before using the EPO online shop to place orders.
- The personal data is stored in the back-end system of the EPO online shop and the EPO's SAP back-end system. The list of Patent Knowledge related products and services is dynamic, and the current status can be found in the EPO website. In certain cases, information in the back-end system may be manually entered by EPO Patent Knowledge staff.
- When needed to handle order processing related issues, personal data are used for identifying the user. To resolve the issue, further personal data provided by the user, might be used.
- To carry out promotion and marketing of EPO products and services. The users may be contacted via the communication channel indicated during the registration process.
- To carry out payment transaction processing for invoiceable products and services, necessary personal data are processed by the relevant EPO departments. The invoicing is undertaken by the Customer Service Centre (CSC) within the Patent Knowledge business area of the EPO, and is based on the information mentioned above. Payment processing is undertaken by the Finance department of the EPO and external service providers.
- For IT support and maintenance, product and service delivery, improvement of the overall service and user experience.

Users may terminate subscriptions by contacting the EPO in accordance with the terms for the relevant products and services, and information will be retained in accordance with this record.

The tools and platforms are integrated across a range of domains, and encompass activities and products / services offered falling under the responsibilities of multiple internal and external processors as further elaborated in this record.

Therefore, in the scope of this activity, the EPO processes personal data for the purposes of:

- Provide a Web Shop frontend for users, order processing, invoicing, user account registration and subscription management;
- Ad-hoc contact with users and marketing;
- Payment transaction processing;
- IT support, delivery and maintenance;
- Service improvement.

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):

- Browsing information: browsing time, cookie information, IP address, website history, and network interaction history;
- Contact information: contact details, country, home address, personal email, phone numbers, working email address;
- Correspondence: personal information provided voluntarily, chat content, additional information which might be provided in the course of exchanges, any other information;
- Education and skills: languages;
- Employment information: company entity;
- Financial: bank account information, bank account number, credit card number, debit card number, VAT ID number;
- Personal identification: first name, full name, gender, nationality, signature, surname;
- User account information: account age, account number, account password.

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 managing 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 Webshop customer ordering a relevant product. These customers may be world-wide.

If necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, Finance, senior EPO management (Observatory on Patents and Technology, VP1 Office, VP4 Office, VP5 Office, President's Office, CGS, MAC) as well as with external contractors providing related processing.

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 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. 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?

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, otherwise contact the delegated data controller at 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 is retained for maximum 7 years. If considered appropriate, data is deleted if it can reasonably be expected that there is no operational need anymore.

Financial data is retained for 10 years, in line with the EPO financial regulations.

Information contained 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.

EPO employees should contact the delegated data controller at PDPatentIntelligence-DPL@epo.org.

Internals may also contact the Data Protection Officer at dpo@epo.org, while externals may contact our Data Protection Officer at 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.