

## **Data protection statement on the processing of personal data in the context of procurement activities**

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.

This privacy statement explains the way in which the EPO processes personal data in the context of the EPO's procurement activities.

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

This data protection statement relates to the processing of personal data during procurement activities.

Companies intending to submit a bid to EPO tenders need to register a user profile on the EPO's eTendering platform. At this occasion a valid business email address must be provided, together with contact details.

Once registered, companies can use the eTendering platform to download procurement documents and enter effectual bids and submit legally valid electronic offers. Offers may contain personal data provided by the company/bidder such as names, contact details, and CVs of employees.

Principal Directorate Procurement and Vendor Management (PD47) processes the data via the eTendering platform to communicate with the bidding companies and to carry out tender procedures.

After winning a bid and a contract, new suppliers need to register to sign up to the EPO procurement and sourcing portal which has been designed to improve partnership and transparency and optimise co-operation between the EPO and its suppliers. During this registration, in addition to company data, an employee of the supplier needs to be assigned for contact purposes and respective data (name, contact details) are to be provided. Contract conclusion involves contract signing electronically via DocuSign integration.

Registered suppliers can use the EPO procurement and sourcing portal to maintain and update the company data and contact details. Additionally, new or amended contracts can be signed or viewed.

PD47 processes the data via the EPO procurement and sourcing portal for concluding contracts and carrying out purchasing activities with suppliers.

On a need-to-know basis, personal data (name, contact details) are made available to EPO Legal (contract conclusion) or EPO Finance (purchasing activities).

The processing is not intended to be used for any automated decision-making, including profiling.

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:

Activities related to eTendering:

Contact Details; Working email address; Job Title Role; Digital Signature; Full Name; Signature; System-, Application-; Additional information which might be provided in the course of exchanges, Security-related Server Logs; Account Password, User ID

Activities related to EPO procurement and sourcing:

Contact Details; Working email address; Job Title Role; ID/Passport picture; National Identity Card Details; Digital Signature; Full Name; Signature; System-, Application-; Additional information which might be provided in the course of exchanges, Security-related Server Logs; Account Password, User ID

Activities related to contract signing electronically via DocuSign integration:

Contact Details; Working email address; ID/Passport picture; National Identity Card Details; Digital Signature; Full Name; Signature; System-, Application-; Security-related Server Logs

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

Personal data are processed under the responsibility of PD 47 Procurement and Vendor Management, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the activities of PD47 referred to in this statement.

External contractors involved in the eTendering platform or the EPO procurement and sourcing portal 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 the EPO Legal and EPO Finance Departments.

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. 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 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?**

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, please write to the delegated data controller at [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org), who is the point of contact for external data subjects. 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?**

The legal basis for processing personal data during activities related to eTendering is Article 5a) DPR which states:

“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”

The processing of personal data during activities related to EPO procurement and sourcing including contract signing electronically via DocuSign integration is Article 5c) DPR which states:

“processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”

Personal data are processed on the basis of the following legal instrument: EPO Financial Regulations, in particular Tender Guidelines and the Directive on Contracts

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

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

Personal data processed during procurement activities will be stored for 12 years

Personal data processed for the verification of the identity in the context of the e-signature are retained for a maximum of 90 days before being erased.

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**

If you have any questions about the processing of your personal data, please 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.