Data protection statement on processing personal data within the procurement procedures of the EPO

Protecting your privacy is of the utmost importance to the European Patent Office ('EPO'). The Office is committed to respecting and protecting your personal data and ensuring your rights as a data subject. All data of a personal nature that identifies you directly or indirectly will be handled fairly, lawfully 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 processes.

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

According to the Financial Regulations, purchasing above a certain threshold must be executed using various competitive procedures or tender processes.
While many competitive procedures still use email to obtain offers from potential suppliers, the eTendering suite of tools is used for tender processes as well as some competitive procedures.
Potential suppliers register for eTendering to download procurement documents and participate in said tender procedures. They can upload their questions and/or bids in the Bidding Cockpit and this data are transmitted electronically back to the Tendering Manager for further processing by the relevant buyer in the EPO procurement department.
The bidders receive automatic notifications to their registered email address informing them when they need to log on to the eTendering platform to see the latest status.

To continue the procurement process, all EPO suppliers have to be registered on the EPO procurement portal which is a cloud-based source-to-pay platform. Companies winning a tender or procedure are requested to register on this procurement portal and enter all their company information including bank details. This system includes the integration with the process for contract signing with a qualified electronic signature by all parties.

Personal data are additionally stored on the shared folder for the creation of documents leading to a final version of a set of tender documents, or later for the financial approval forms and assessment and awards reports. After a procedure has been finalised, the resulting contract is also stored on this folder with all its drafts and approval documentation.

All procedures above €200k are also recorded in "Extend" which is an excel-based file stored on a share drive. This tool is used to report to management and keep track of bigger exercises and all details needed to track the lifecycle of the procurement processes are stored.
That includes the description of the procedure, the buyer ID who initiated it, the EPO employee involved in its running, the department that requested it, amount and dates for different milestones of the procedure and data about external companies that submitted offers. The data is filled in by the buyers and is accessible only to the staff in Procurement.
Personal data are processed for the following purposes:

- To manage tender and procurement procedure.
- To inform EPO buyers that potential bidders have submitted questions and contact them during the process of an active tender procedure.
- To collect feedback from bidders so that the controller can deliver better and more effective tender documents, according to bidders' needs.
- To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents.

2. What personal data do we process?

Depending on the system, the following categories of personal data are processed.
Mandatory personal data is collected to create the user account in the eTendering:

- First name and last name
- Business email address
- Business phone number
- Business address details
- User ID
- Password
- Business entity
- Job title role.

The following data is produced by the system based on a user's activity:

- EPO tenders enrolled in,
- first access to EPO eTendering (date and time)
- last access to EPO eTendering (date and time)
- Logs, user connection data (such as IP, date, time)
- Completion results and date of completion.

Procurement portal:

- First name and last name
- Business email address
- Business phone number
- Business address details
- User ID
- Password
- Job title role.

Signature-process tool:

- ID/Passport picture
- National Identity Card Details
- Passport number
- Facial recognition
- Business email address
- Business entity
- Job title role
- Signatures (qualified electronic signatures)

Generally, companies' data are registered, rather than personal data.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the 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 initiative, project or activity of referred to in this statement.

External contractors involved in internal IT staff and external contractors, may also process personal data.

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

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.

Personal data is disclosed on a need-to-know basis to the EPO staff working in Procurement and Vendor management department. The EPO BIT department and the Finance departments, as internal processors, have access to the data as well as the external contractor involved in the processing activity (such as the contractors involved in maintaining the EPO It system may also have access to relevant personal data).
Additionally, an internal database has been created to share information on i.e. bids, contract drafts, assessment and award reports etc. to EPO internal stakeholders that might have interest in the tender.

5. How do we protect and safeguard your information?

We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.
All personal data are stored in secure IT applications according to the Office's security standards. These include:

- User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication;
- Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum;
- Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices
- Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices;
- Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk;
- Security incidence response: 24/7 monitoring for incidents, on-call security expert.

For personal data processed on systems not hosted on EPO premises, the providers processing the personal data for the contract management and signature processes 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 your personal information and, if necessary, correct it? How can you receive your data? How can you request that your personal data be erased, or restrict or object to its processing?

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 PDCProcurement-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 are processed on the basis of Article 5 (a) and (b) DPR, which say:

a) *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, or*
b) *processing is necessary for compliance with a legal obligation to which the controller is subject, or*

The special categories of personal data are processed on the basis of Article 11(2)(f) DPR, which allows the processing when is "*necessary for a specific purpose relating to 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 substantially necessary for the management and functioning of the Office, having regard to the principle of proportionality, or in reason of obligations arising from its duty of co-operation with the contracting states. This processing shall be based on a legal instrument which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".

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

8. How long do we keep your data?

In the eTendering platform, bidders can delete their company registration if they so wish once the procedure(s) they participated in has been set to completed. Employee information can be deleted at any time as long as there is still one employee registered for participation in an open procedure. User administrator can delete personal data upon request.

Personal data processed for the contract management and the e-signature process will be kept as long as the contract with the provider is in place and feature are available to close users' profiles upon requests. 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.

9. Contact information

If you have any questions about the processing of your personal data, externals should contact the DPO and/or the delegated data controller at DPOexternalusers@epo.org. please write to the delegated data controller at PDCProcurement-DPL@epo.org.

You can also contact our Data Protection Officer at dpo@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.