Data protection statement on the processing of personal data in the scope of the EPO Legal Interactive Platform

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.

Introduction

This data protection statement specifically pertains to the processing of personal data done in the scope of the service EPO Legal Interactive Platform, which is offered to selected MyEPO.org users as an option in their portfolio of functionalities.
The EPO Legal Interactive Platform is an EPO chatbot which empowers users to guide conversations towards specific levels of detail on subjects related to legal topics within the legal sources listed below. Through successive prompts and replies, users can fine-tune the context of their discussions. To facilitate users returning to prior conversations, the Legal Interactive Platform retains the history of interactions for each user; users can permanently delete own past interaction history at any time. The user can express an opinion in the form of a feedback regarding the quality of the answer received and in case of negative feedback he is allowed to include a feedback comment to help improving the tool. Feedback, both positive and negative, will be used for further tuning and improvements.
The tool is designed to provide information and answer questions specifically about the European Patent System.
Users of the EPO's Legal Interactive Platform are invited to enter in the chatbot's prompts exclusively information that is available in the public domain.

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

The processing operation consists in collecting and sending the user's prompts entered into the chatbot's user interface and in storing the user's past chat history into a database (hosted on Azure Cloud) along with the User ID which has been hashed and truncated.
Prompts that do not lead to a completion (i.e. to an answer from the LLM - Large Language Model) are not stored in the database; all other prompts are stored with the User ID hashed and truncated exclusively to enable retrieval.
The purposes of processing are:

- to answer user's queries about the European Patent System, also by means of user's subsequently refined prompts;
- to facilitate the user carrying on a conversation with the chatbot by retaining and leveraging the user's past interaction history;
- to improve the accuracy of EPO's Legal Interactive Platform service by analysing the saved prompts; the user ID of the user who has entered a given prompt and/or feedback is pseudonymised by means of hashing and truncation;
- to identify, troubleshoot and fix anomalies and incidents affecting the service;

- to derive anonymised statistics about most searched topics.

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: User ID, browser User-Agent, browsing date and time, IP address, cookie information, prompts entered by the user, user's feedback and feedback comments, answers provided to the user by the service, user's past interactions history, session-related information, voice input (foreseen in next releases), system logs.

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of PD4.5 Chief Technology Officer, acting as EPO's delegated data controller.

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
- 4.5.1.3 BIT Data Science for the purpose of analysing users' prompts, feedback and comments;
- 4.5.3.3.1 BIT Front Office Tools product team for the maintenance of the service.

Personal data may be disclosed to third-party service providers, i.e. external contractors for maintenance and support purposes.
Personal data will only be shared with authorised personnel 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.

All personal data processed in the systems are stored in secure IT cloud application according to the security standards of EPO.
These include:
- User authentication: myEPO.org users are identified and authenticated via EPO's Customer Identity and Access Management system (CIAM); EPO personnel workstations and EPO servers require login, 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 between administrative and user roles, users have minimum

privileges, reduction of overall administrative roles to a minimum.
- Masking: User IDs are hashed and truncated to prevent user re-identification.
- Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, antivirus 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 incident response: 24/7 monitoring for incidents, on-call security expert.

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). The right of rectification can only apply to inaccurate or incomplete objective and factual data processed and does not apply to subjective statements.

If you would like to exercise any of these rights, please write to the delegated data controller at DPOexternalusers@epo.org ; 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), 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 (aa) DPR: the processing is necessary for the management and functioning of the EPO.

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.
Logs are kept for up to three months.
User's chat history is kept for up to three years; the user has the ability to delete it at any time.
User feedback is retained for up to three years.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at DP_BIT@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.