Data protection statement on the processing of personal data in the context of User Experience (UX) research on EPO software applications

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.

UX design, or User Experience design, is a multidisciplinary field focused on creating user-centric products, services, and systems. Starting from ergonomics, UX design encompasses the entire user journey when interacting with a product or service.
At the Office, UX design ensures the EPO's tools are not only functional but also user-friendly, making navigation seamless and tasks efficient for patent examiners and legal professionals.
The EPO's UX philosophy hinges on user-centricity, accessibility, and continuous improvement.
BIT 4514 User Experience department strives to understand end-users' unique challenges, translating this understanding into intuitive application interfaces and streamlined processes; at the European Patent Office, UX design is a collaborative journey that involves everyone, including first and foremost the end users.
The best insights come from those who use the EPO's systems daily; their valuable feedback and active participation play a vital role in shaping the EPO's UX enhancements.

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

This data protection statement relates to the processing of personal data done in the context of User Experience (UX) research on EPO software applications.

BIT 4.5.1.4 User Experience team collects and processes quantitative and qualitative data from application end-users. The purpose is to get statistically solid, representative figures about user satisfaction with EPO products and services.
To this end, the UX team applies various methods and tools such as:
• generative research methods with the purpose of identifying user needs especially but not exclusively: user interviews, surveys, diary studies, and any other method usually used for the purpose of identifying user needs; any method for achieving that purpose can be conducted either in person or via digital means;
• evaluative research methods with the purpose of validating design solutions and ideas especially but not exclusively: usability testing, prototype testing, A/B testing, and any other method usually used for the purpose of validating design solutions and ideas; any method can be conducted either in person or via digital means;
• analysis of user feedback and data extracted from analytics tools especially, but not exclusively: from Matomo (see https://matomo.org/features/), from customer support platforms (e.g. ServiceNow), or other user channels, (e.g. MS-Teams chats), and from any other tool usually used for the purpose of collecting user feedback and data.
By means of all the above, UX design empowers EPO applications' end-users, enhances productivity, and supports the European Patent Office's mission.

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 may be processed, for EPO employees and for externals:

- personal identification: first name, last name, full name, disability or specific condition;
- contact information: work email address;
- (for EPO employees only) EPO site;
- employment information: department name and/or number, job title role, preferred language of communication; (for EPO employees only) line reporting manager, duration of employment, office location;
- user account information: application-specific user role;
- data about the representation in EPO's Patent Granting Process: role in the Patent Grant Procedure;
- correspondence data: chat content, additional information which might be provided in the course of exchanges, personal information provided voluntarily and/or any other information;
- physical and/or digital identifiable assets: operating system version;
- answers to surveys, assessment or quizzes;
- ticket-related data;
- browsing information: IP address, network interaction history, navigated URL, Referred URL, files clicked and downloaded, outlink (i.e. links to an outside domain that has been clicked), page title, page generation time, category, browsing time, website history, browser User-Agent, browsing date and time, search query, cookie information;
- user geolocation information: country, region, city, approximate latitude and longitude;
- sensory and electronic information: visual information and audio information (kept temporarily only to provide support during testing and interviews).

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Chief Technology Office Principal Directorate PD4.5, acting as the EPO's delegated data controller.

Personal data are processed internally by members of BIT 4.5.1.4 User Experience and of BIT 4.6.

External contractors - that are involved in providing communication platforms, ticketing services, UX design platforms and UX consultancy - may also process personal data, which can include accessing it.

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

Recipients of the personal data processed in the present processing operation are the staff in EPO 4.5.1.4 User Experience, in PD4.6 and the Director of 4.5.1. Enterprise Architecture.

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.
Specific members of 4.5.1.4 UX team are granted permission to record interviews/testing sessions with EPO users, according to their specific role, assignment and need-to-know; such permissions are checked and either revalidated or revoked on annual basis.

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.

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 DP_BIT@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 DPR Article 5 (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.

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 will be deleted after 3 months since their collection. By the end of the retention period, anonymised reports are created and original personal data are deleted for good.

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 are an EPO internal and 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.

If you are an external and have questions about the processing of your personal data, please write to the DPO 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.