Data protection statement on the processing of personal data in the context of the EPO external communication website ("epo.org")

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 explains the way in which the EPO collects and process personal data when you use the EPO website ("epo.org").

For instance, it is used by the EPO to contact users requesting information or support related to EPO activities and events (such as the website feedback, the "Press Call Back" services, the Discussion Forums section publication of audio-visual material related to the EPO's activities), to handle the event and webinar management services, including audience management (e.g. registration for EPO webinars, online conferences, training and public events) as well as providing information regarding patent products and patent granting procedure (such as, the "find a professional representative" function, the oral proceedings calendar or the publication of specialised information for the journalist related to EPO services, activities and events).

Personal data are processed for the following purposes:

- to maintain basic technical services of the EPO website, including the processing of users' personal data for provision of enhanced web services
- to contact users requesting information or support with regards to EPO activities, services or events
- to manage certain services related to the patent granting processes
- to collect feedback
- to promote EPO's activities and events

Additional services accessible via the EPO website or activities organised and managed by the EPO might require the processing of personal data for other and further purposes.

For more information about those processing operations

please consult the dedicated data protection statements available on the Data protection page on the EPO website.

We do not have social plug-ins for epo.org, however we use social media to communicate our work and better engage with the public. On the epo.org you might find services or links related to those platforms. Please bear in mind that if you use the services or access the social media via epo.org, the social media provider might process personal data about you. Each social media provider has its own policy on how it processes your personal data when you access its website. We therefore encourage you to refer to the various providers' privacy policies for more information on the purposes and scope of their processing of the personal data.

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).

The processing activity may leverage the use of artificial intelligence (AI) in certain systems, and applications supporting the operation of epo.org. AI functionalities may be used to improve user experience, support website administration and maintenance, enhance security monitoring, and facilitate the delivery of information and services. The deployment and use of AI in this processing activity adheres to stringent requirements in the processing of personal data.

2. What personal data do we process?

The following categories of personal data are processed:

General web analytics information

- date and time of the request
- title of page being viewed (page title)
- URL of page being viewed (page URL)
- URL of page that was viewed prior to the current page (referrer URL)
- screen resolution used
- files that were clicked and downloaded
- links to an outside domain that were clicked
- pages generation time (i.e. the time it takes for webpages to be generated by the webserver and downloaded by the user)
- main language of the browser used (accept-language header)
- user agent of the browser used (user-agent header)
-

EPO employees (providing editorial access)

- first name and surname
- professional email address

For epo.org users

- title, if applicable
- first name and surname
- country of residence, if applicable
- email address (personal and/or professional)
- postal address (personal and/or professional), if applicable
- telephone/mobile number (including country code) (personal and/or professional), if applicable

- fax (including country code), if applicable
- statements, comments and opinions shared in the additional/feedback/background comment sections or discussion forums
- preferred language of contact
- contact details from professional representatives or participants in oral proceedings
- enquiry description and/or reference numbers and any statements/comments and/or opinions shared as part of the information exchange between the EPO and the user
- additional information requested depending on the nature of the processing operation

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Principal Directorate Communication ("PD Communication), 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 PD Communication and Business Information Technology ("BIT") business units referred to in this statement.

External contractors involved in providing a platform or 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?

Personal data are disclosed on a need-to-know basis to the EPO staff working in PD Communication, BIT Online Solutions and BIT Security.

However, please bear in mind that some online tools and services available on the EPO website (e.g., contact forms or patent granting and related procedures) may be under the responsibility of different organisational units. In that case, for further information on the processing of your personal data please refer to the applicable data protection statement for the specific online form.

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

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 pdcomm-dataprotectionliaison@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 (depending on the data subjects concerned, please include all the applicable forms: form (for externals), form (for internals) and/or form (for pensioners)) 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 in accordance with Article 5 a. and d. DPR:

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

d. the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes (e.g., including profile pictures to their profiles).

8. How long do we keep your data?

Please note that, in cases where the personal data is collected by other organisational units via the epo.org, they will be stored and deleted according to the applicable and respective retention period(s) determined by the delegated data controller, i.e.: the relevant organisational unit.

Personal data will be kept only by PD Communication for the time needed to achieve the purposes for which it is processed and then deleted from its databases as follows:

Personal data related to editorial access will be deleted once the user leaves the office or switches to a role that no longer requires editorial access.

Information obtained via the web analytics is stored and deleted after a maximum period of 10 years

Personal data related to contact details (e.g.: name, surname, email address, affiliation) are stored for a maximum period of 5 years and subsequently deleted.

This 5-year retention period only refers to contact details processed within the scope of this DPS, such as contact information collected through communication-related enquiries, subscriptions, stakeholder engagement activities or similar interactions. It does not apply to personal data processed under separate DPSs, which may be subject to different retention periods.

Personal data featured in press releases and other external publications (e.g.: PD Communication newsletters) will be stored and deleted after 10 years.

Personal data related to events, conferences and meeting agendas will be stored and deleted after 3 years.

Personal data contained in photographs, video and audio-visual recordings created as part of meetings, events or other initiatives are retained in accordance with the applicable retention criteria. For multimedia content managed by PD Communication, the applicable criteria are set out in the PD Communication Multimedia Retention Policy, which complements the EPO Retention Policy and provides guidance on the retention, management, storage and lifecycle of such content. In this sense, depending on the nature and purpose of the meeting, event or initiative, including its educational, institutional, historical, informational or promotional value, multimedia content may generally be retained for periods of 2, 10 or 25 years, in accordance with the applicable retention category. The Multimedia Retention Policy is available upon request.

Content published on EPO general website (e.g. corporate multimedia material) and integrated pages will be stored and deleted after 10 years as of the date when the document is archived from the website.

As for personal data related to tracking information, it will be stored and deleted according to the relevant cookie policy in place for the event, if applicable.

In the case 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 write to the delegated data controller at pdcomm-dataprotectionliaison@epo.org.
You can also contact our Data Protection Officer at DPOexternalusers@epo.org.mailto:dpo@epo.org

10. Cookie policy

For further information on the use of the cookies when accessing epo.org website, please refer to the cookie policy available on the website and accessible via this link.

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.