

Data protection statement¹ on the processing of personal data within the context of the administration of general authorisations

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.

Representation in proceedings with the EPO may be undertaken by professional representatives registered on the list of professional representatives before the EPO as well as by legal practitioners and employees upon the fulfilment of specific legal requirements. Legal practitioners and employees must always file an authorisation with the EPO, while professional representatives must file an authorisation under specific circumstances only. Instead of filing an individual authorisation in each case of representation, representatives may file a general authorisation enabling them to act in respect of all patent transactions before the EPO. Principal Directorate 5.2 Legal Affairs (PD 5.2), specifically the Legal Division of the EPO (within Directorate 5.2.3), register and administer these general authorisations, which necessarily involves the processing of personal data to which this data protection statement relates.

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

General authorisations are received by PD 5.2 Legal Affairs by post or are filed in an in-house application. The requestor (usually the authorisor) provides personal data such as name, address and other specific information (of the authorisor and authorisee) and appropriate evidence as required, such as proof of employment. Initial checks are made to verify the existence of the authorisor and authorisee, and to categorise the request as a new authorisation or as an amendment to an existing authorisation. After processing of the request for general authorisation, confirmation letters are distributed either to the employee or to the authorisor if so requested. The general authorisation including the scope of rights awarded is registered in the EPO's internal database, including personal data of the authorisee and authorisor. General authorisations are also stored in a paper archive.

Personal data are processed for the purpose of the administration of general authorisations and providing up-to-date information to stakeholders, as well as all for associated actions, e.g. to ensure a proper and efficient information flow and effective management of associated activities. This encompasses:

- (i) registration and deletion from the list of general authorisations and use of this information by the EPO for related actions during the patent granting process
- (ii) providing EPO units with information necessary to perform tasks associated with general authorisations
- (iii) preparation of statistics

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

¹ Version June 2022

protection, such 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 types/categories of personal data can be processed regarding external data subjects, including authorisers and authorisees:

- personal identification and contact data (such as name, email address, phone number)
- data related to representation in the EPO's patent grant process (including supporting documentation, role in the patent grant procedure, affiliation to an association of professional representatives, authorisee/authoriser function)
- employment information (job title, company entity, representative registration number (ID))
- ticketing (ticket-related data)

The following types/categories of personal data can be processed regarding EPO employees involved in the administration of general authorisations:

- personal identification and contact data (such as name, email address)
- employment information (such as location, personnel number, job title)
- ticketing (ticket-related data)

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Principal Director of Legal Affairs acting as the EPO's delegated data controller.

Personal data are processed by PD 5.2 staff involved in the administration of general authorisations.

External contractors involved in maintaining services necessary for the administration of general authorisations, including Microsoft and ServiceNow, can also process personal data, which may include accessing it.

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

PD 5.2 employees of the Legal Division have access to personal data.

Personal data are disclosed on a need-to-know basis to the following units:

- DG0 President's Office
- DG1 Patent Grant Process
- DG5 Legal and International Affairs.
- other parties may also be granted access, such as the Board of Appeals on a need-to-know basis in appeal cases

Personal data may be disclosed to third-party service providers for the maintenance of services necessary for the administration of general authorisations, including Microsoft and ServiceNow.

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 restricted access.

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), unless the EPC, the PCT or any practices or provisions applicable under them require otherwise in relation to personal data processed in patent granting and related procedures (see the [Decision of the President](#) of 13 December 2021, OJ EPO 2021, A98).

The right to rectification can only apply to inaccurate or incomplete factual data processed in the context of the EPO's tasks, duties and activities; it does not apply to subjective statements, including ones made by third parties. The right to erasure does not apply where the legal obligation on the controller (e.g. to manage the administration of general authorisations (Article 1.1(d), Decision of the President of the EPO concerning the responsibilities of the Legal Division, OJ EPO 2013, 600)) requires the processing of personal data.

If you would like to exercise any of these rights, please write to the delegated data controller at DPOexternalusers@epo.org if you are an external data subject. EPO employees can contact PDLegalAffairs-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 receiving it. 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 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
- (b) processing is necessary for compliance with a legal obligation to which the controller is subject (e.g. to manage the administration of general authorisations as per Article 1.1(d), Decision of the President of the EPO concerning the responsibilities of the Legal Division, OJ EPO 2013, 600)

Personal data are processed on the basis of the following legal instruments:

- Article 133 and Article 134 EPC
- Rule 152(4) EPC
- Decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division (OJ EPO 2013, 600)
- Decision of the President of the European Patent Office dated 12 July 2007 on the filing of authorisations (OJ EPO 2007, Special Edition No. 3, 128)

8. For how long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which they are processed. In light of the purposes of the processing, it is necessary for data to be retrievable in case of issues with regard to a procedure or the activities of professional representatives. All data, in particular the information on who acted in the functions of authorisor and authorisee, must therefore be retrievable until all individual and general authorisations have lapsed.

Specifically, personal data will be stored/deleted on the following basis:

- If a general authorisation is withdrawn, its status becomes inactive in the system. Related personal data will be deleted 99 years after the withdrawal.
- When a function/mandate as authorisor or authorisee is withdrawn from a general authorisation, the corresponding status of that data subject becomes inactive. Relevant personal data are destroyed when the general authorisation reaches the end of its retention time.
- A general authorisation and the information on who acted in the related functions of authorisor and authorisee, together with related personal data, are destroyed at the latest 99 years after the last authorisee has been withdrawn from the list in which they were registered (e.g. as a professional representative, legal practitioner etc).

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 write to the delegated data controller at DPOExternalUsers@epo.org if you are an external data subject, or to PDLegalAffairs-DPL@epo.org if you are an EPO employee.

Internals may also contact our Data Protection Officer at dpo@epo.org, while externals may contact our Data Protection Officer 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.