

Data protection statement¹ on the processing of personal data related to pre-litigation and litigation on civil service matters where the Administrative Council is the competent appointing authority

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.

Pre-litigation and litigation on civil service matters where the Administrative Council is the competent appointing authority might require the processing of personal data by Principal Directorate 5.2 Legal Affairs (PD 5.2), to be able to advise, assist and possibly represent the appointing authority in the proceedings. This data protection statement relates to the personal data processed during these activities.

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

This data protection statement explains the way in which personal data are processed when assisting and/or representing the Administrative Council in civil service pre-litigation and litigation cases. The nature of the processing operations varies depending on the specifics of a case, but will usually involve collecting and recording data for use in proceedings. Personal data may also be disclosed, for example, to external law firms assisting with delivering the services or as part of the relevant proceedings.

Personal data are processed for the purposes of the EPO's administrative functioning, in particular:

- to assist and/or represent the Administrative Council throughout administrative or judicial proceedings initiated against its decisions;
- to ensure the availability of dispute files for later reference in the event of subsequent litigation;
- for archiving and statistical purposes.

2. What personal data do we process?

The following types/categories of personal data are (or might be) processed:

- role in the matter (e.g. claimant, representative, expert, witness) and associated information;
- personal identifying data, including contact details (e.g. name, email);
- information on the case at hand and related documents, in particular:
 - o case reference;
 - o information related to the data subject to whom the case relates, such as employment information (e.g. date of birth, nationality, employment start date, grade, position held), past grievances and complaints, appeals record;
 - o challenged decision and claims against it;
 - o information related to the substance of the matter, which, depending on the topic, might include personal data of a sensitive nature (e.g. disciplinary measures, health-related data, trade union membership);
 - o correspondence, including requests, opinions, decisions and, in the case of litigation, pleadings, submitted documents and witness statements.
- ticket-related information (Case Management System)

¹ Version April 2023

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of PD 5.2 Legal Affairs acting as the EPO's delegated data controller.

Personal data are processed by EPO staff who are involved in the activities referred to in this statement, in particular staff from Directorate 5.2.3 Institutional Law, Legal and Unitary Patent Division. Personal data are also processed by EPO staff from Directorate 4.4 General Administration (language services), e.g. for translations.

External contractors involved in providing and maintaining tools and services necessary for the activities described above, such as Microsoft, OpenText, and Thomson Reuters, may also access and process the personal data.

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

EPO staff in Directorate Institutional and Contract Law have access to the personal data described above.

Personal data may also be disclosed on a need-to-know basis to EPO staff in other departments for information and/or consultation, e.g. to the Chairperson and Secretariat of the Administrative Council, to the EPO hierarchy (VP 5 assisted by the CILO, President of the Office), to PD 4.2 People (Human Resources), to PD 0.8 Employment Law and Social Dialogue Advice, to the Boards of Appeal Unit, to the Ombuds Office and to D 0.4.4 Ethics and Compliance.

Personal data may be disclosed on a need-to-know basis to the staff member(s) of the unit(s) involved in the prevention and settlement of legal disputes (whether in internal, judicial or alternative redress mechanisms afforded by the EPO or any other legal processes involving the EPO), when this is necessary and proportional for them to perform tasks carried out in the exercise of their official activities, including representing the EPO in litigation and prelitigation. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and with the principles of confidentiality and accountability.

[Personal data may be disclosed on a need-to-know basis to staff in the unit or units involved in preventing and settling legal disputes (whether as part of internal, judicial or alternative redress mechanisms afforded by the EPO or of any other legal processes involving the EPO) if this is necessary and proportional for the purposes of performing tasks carried out in the exercise of their official activities, including representing the EPO in litigation and prelitigation. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and with the principles of confidentiality and accountability.]

Personal data may also be shared on a need-to-know basis with external attorneys at law.

Personal data may be disclosed to third-party service providers, such as Microsoft, OpenText, and Thomson Reuters, for the provision and maintenance of tools and services necessary for the activities described above. These third-party service providers may also access and process the personal data.

Personal data will only be shared with authorised persons responsible for the necessary processing operations and 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 a restricted access.

For personal data processed on systems not hosted on EPO premises, the EPO has carried out a privacy and security risk assessment. 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.

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 and you are:

- an external user, write to our Data Protection Officer at DPOexternalusers@epo.org.
- an EPO staff member, write to the delegated data controller at 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 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.

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 requires the processing of personal data. With regard to the right of access, certain information may be deleted from the copy of personal data provided to the data subject if the EPO considers it necessary in the interest of protecting the confidentiality of internal deliberations and decision-making,

Restrictions of data subject rights can occur as the result of Circular No. 420, Article 4(1)(c): “pursuant to Article 25(1)(a), (b), (c), (e), (f), (g) and (h) DPR when processing personal data (...) in connection with the establishment, exercise or defence of legal claims involving the EPO or its subordinate bodies, including arbitration, in order to preserve confidential information and documents obtained from the parties, interveners or other legitimate sources”.

7. What is the legal basis for processing your data?

Personal data are processed on the basis of Article 5 DPR. Accordingly, personal data are processed when:

- (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; or
- (b) processing is necessary for compliance with a legal obligation to which the controller is subject.

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

- Article 13 of the European Patent Convention;
- Articles 106-113 Service Regulations;
- Implementing Rules for Articles 106-113 of the Service Regulations;
- Article 18 of the Rules of Procedure of the Administrative Council.

8. 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.

After the closure of a matter, related files will be kept for 20 years.

An index of cases with limited personal data categories (e.g. reference, name, status) is kept for ten more years to track workflows as well as for statistical purposes. Possible archiving activities are addressed in a separate data protection statement.

In the event of a formal appeal/litigation on data protection grounds, all data kept on file when the formal appeal/litigation was initiated will be kept until those proceedings regarding data protection have been concluded, or for the period described in the data retention policy above, whichever is longest.

9. Contact information

External data subjects who have any questions about the processing of their personal data should contact the Data Protection Officer at DPOexternalusers@epo.org. EPO staff should contact the delegated data controller at pdlegalaffairs-dpl@epo.org. They may also contact the 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 a 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.