Data protection statement on the processing of personal data within framework of the Internal Appeals Procedure

Protecting your privacy is of the utmost importance to the European Patent Office ('EPO' or 'the Office'). 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.

The delegated controller's involvement in the Internal Appeals procedure and the corresponding collection (and processing) of personal data is triggered by the file of an internal appeal by (an) EPO employee(s) to the Internal Appeals Committee (ApC). The ApC notifies the delegated controller of its obligation to provide submissions necessary for the processing of the internal appeal and sets a deadline to reply.

For the Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers to prepare the Office's defence and draft the submissions to the ApC, personal data stored in the internal appeal file is processed. The internal appeal file mainly comprises personal data collected from the pre-litigation procedure (i.e. the management review procedure as provided for in Article 109 ServRegs). In some cases, the personal data has already been collected during previous dispute settlement procedures as envisaged under Article 106-113 ServRegs. The data is stored electronically.

Additional data is collected from the appellant's submissions and during the fact-finding exercise prior to drafting the position paper. PD08 Lawyers may contact other business units, including the line manager of the appellant where necessary for information or fact-checking purposes concerning the internal appeal. Personal data obtained through this fact- finding exercise or through Office-wide databases may be processed for the drafting of the Office's submissions.

Additional information may be processed when answering a request for information from the ApC or when carrying out a settlement initiative.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to the ApC.

PD08 Lawyers draft submissions electronically. The submission is sent to the Appeals Committee Secretariat via email by the Employment Law Secretariat. This submission, having been paginated by the Appeals Committee Secretariat, becomes part of the official appeal file.

PD08 lawyers may attend a hearing held by the ApC for the deliberation of the case. The lawyer defends the Office's position and may provide oral submissions. The employee(s), possibly represented by a lawyer, shall also be present at the hearing and defend their case before the ApC.

The delegated controller's involvement in the issuance of a Final Decision is triggered by the receipt of a reasoned opinion from the ApC pursuant to Article 110 ServRegs.PD08 is informed of the opinion of the ApC which becomes part of the appeal file stored in MatterSphere and serves as the basis for the preparation of the Final Decision pursuant to Article 110(4) ServRegs.

In order to prepare a Final Decision, the personal data included in the appeal file is processed. PD08 Lawyers process the ApC opinion and prepare a Note to the relevant authority explaining the facts of the case, the ApC opinion and the recommended Final Decision.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member initiates an appeal in front of the ApC.

The processing of personal data is necessary in order to address all aspects related to the internal case file (fact-finding), the consequences of the Final Decision, the creation of statistics, lists and the legal analysis, if necessary.

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

This data protection statement relates to the processing of personal data of data subjects in the handling of an internal appeal and representing the Office's position for assessment by the ApC, concluding the internal appeals procedure and issuing a final decision in accordance with Article 110(4) of the Service Regulations and the creation of statistics and legal analysis, if necessary.

Personal data are processed for the following purposes:

- The fulfilment of the internal appeals procedure under Article 110 Service Regulations.
- Providing PD08 Lawyers with an understanding of the appellant's grievance and the surrounding circumstances.
- Establishing all of the facts to provide comprehensive submissions to the ApC on the Office's behalf.
- Identifying cases that may be suitable for amicable settlement.
- Providing the ApC with adequate information to enable the presiding Committee members to deliver a reasoned opinion.
- Providing the hierarchy / relevant authority with adequate information on the case to enable them to make an informed, fair and balanced decision.
- The reassessment of a case depending on the ApC opinion.
- Issuing and executing the Final Decision.
- Contacting the appellant(s) and notifying them of the Final Decision.
- The monitoring of deadlines.
- Identifying recurring and systemic legal issues.
- On request, the preparation of statistics and lists for the hierarchy.
- The preparation of legal analysis for hierarchy and other business units to identify trends and assess the effectiveness of legal arguments over time.
- Providing an archive of legal reference for lawyers.

The processing is not intended to be used for any automated decision-making, including profiling.

2. What personal data do we process?

The following categories of personal data are processed:

(i) Appellant(s): The data provided is strictly necessary for the purpose. Depending on the case and the need for the defence, preparation and implementation of the Final Decision, various details about the individuals may be processed such as:

- Identification details: name, surname, date of birth, nationality, marital status, encrypted bank details (on a strictly need-to-know basis for the adjudication of the case).
- Professional details: department, grade and step within department, years of service, employment status (active/inactive/retiree), allowances received, rewarding history, remuneration, engagement in additional tasks, professional contact details.
- Litigation history (re past and pending disputes) if relevant for the case.
- Any statements relating to the case.
- Depending on the subject matter of the litigation, it might require the processing of special categories of data or of sensitive data, such as:
    - Health information
    - Sex life or sexual orientation (especially in cases involving allegations of harassment or discrimination)
    - Trade union membership
    - Criminal offences, criminal convictions
    - History of any disciplinary measures or sanctions against the appellant.

  Such processing takes place on a strict need-to-know basis, only as necessary for the adjudication of the case.

(ii) Appellant's legal representative / successors:

Personal data may be processed such as:

- Identification details: Name, surname, signature.
- Professional Details: Title/Position within the firm, professional contact details.
- Their legal statements and other communications.

(iii) PD08 Lawyer:

Personal data may be processed such as:

- The Identification details: name, surname, signature.
- Professional Details: Title/Position and department within the EPO, professional contact details.
- Their legal statements or other communications.

(iv) Individuals mentioned in the submissions:

Personal data may be processed such as:

- Any information related to them in the submissions.
- Their own statement, which can be required by the Office.

(v) Witnesses/experts during a hearing and/or in the submissions:

Personal data may be processed such as:

- The Identification details: name, surname.
- Professional details: Title/Position and department within the EPO, professional contact details.
- Their own statements.

(vi) Employment Law Secretariat:

Personal data may be processed such as:

- The Identification details: name, surname.
- Professional details: Title/Position and department within the EPO, professional contact details.

(vii) Appeals Committee Secretariat:

Personal data may be processed such as:

- The Identification details: name, surname.
- Professional details: Title/Position and department within the EPO, professional contact details.

(viii) Members of the Appeals Committee:

Personal data may be processed such as:

- Identification details: name, surname (signature) of the members.
- Correspondence as well as their requests, opinions, procedural decisions.

(ix) Competent Authority:

Personal data may be processed such as:

- Identification details: name, surname (signature).
- Professional details: Title/position and position within the EPO, professional contact details.
- Correspondence and decision.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Principal Directorate Employment Law and Social Dialogue Advice (PD08), 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 the ApC, the competent authority taking the decision and other internal operational units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, and whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as:

(i) the provision of information on the requested information during the fact-finding exercise before the ApC.
(ii) the execution of the ApC opinion and subsequent final decision, and the reassessment of a case depending on the ApC opinion.
(iii) the preparation of statistics and lists if necessary.

External contractors involved in providing a platform and/or maintaining certain services such as Microsoft (Office, Exchange, Outlook, Teams), OpenText and Thomson Reuters (MatterSphere) 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 the Principal Directorate Employment Law and Social Dialogue Advice (PD 08) in order to perform tasks carried out in the exercise of the official activities and that are necessary for the management and functioning of the PD 08. Personal data are further disclosed on a need-to-know basis to:

a. Members of the ApC and the Appeals Committee Secretariat.
b. The appellant's legal representative / successors where they are engaged in the litigation.
c. Witnesses/experts.

Personal data are disclosed on a need-to-know basis to the EPO staff working in other operational units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as:

(i) the provision of information on the requested information during the fact-finding exercise before the ApC.
(ii) the execution of the ApC opinion and subsequent final decision, and the reassessment of a case

depending on the ApC opinion.

(iii) the preparation of statistics and lists.

Personal data may be disclosed to third-party service providers for maintenance and support purposes (e.g., Microsoft (Office, Exchange, Outlook, Teams), OpenText and Thomson Reuters (Matter Sphere)).

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.
These include:

- User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, 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 into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum;
- Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV 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 incidence 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).

The right to rectification only applies to inaccurate or incomplete personal data processed. Your right to rectification applies only to factual data processed as part of the appeals procedure.

If you would like to exercise any of these rights, please write to the delegated data controller at pdemploymentlaw&socialdialogueadvice-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 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.

Please note that, your rights may be subject to restrictions outlined under Circular 420 Implementing Article 25 of the Data Protection Rules.

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

Personal data are processed on the basis of Article 5 (a) DPR: It is necessary for the performance of a task carried out on the basis of legal provisions of the European Patent Organisation or in the legitimate exercise of the official authority vested in the EPO.

Processing is necessary for the performance of the settlement of disputes as foreseen by Title VIII Articles 106-113 of the Service Regulations and its Implementing Rules. Article 110 ServRegs provides for the conditions under which a staff member can submit an internal appeal to the ApC.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data. In such a case, personal data are processed on the basis of Article 11(2)(b), (e), (f) and Article 11(3) DPR.

Depending on the subject matter of the proceedings, it might require the processing of personal data relating to criminal convictions and offences. In such a case, personal data are processed on the basis of Article 12(1) DPR: The processing is covered by legal provisions of the European Patent Organisation providing for appropriate safeguards for the rights and freedoms of data subjects.

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 concerning the appeals procedure will be stored until the last day of the 20th calendar year following the issuance of the final decision.

The retention time applies to both electronic and paper files.

In the event of a complaint before ILOAT, all data held at the time the complaint was lodged will be retained until the proceedings have been closed. Reference is made to the retention periods in complaint procedure before the ILOAT described in the relevant DPS.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at pdemploymentlaw&socialdialogueadvice-dpl@epo.org.

You can also 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.