Data protection statement on the processing of personal data in the handling of Data Protection Board (DPB) complaints

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 involvement of the Principal Directorate Employment Law and Social Dialogue Advice (PD 08) in the complaint procedure before the Data Protection Board ('DPB') and the corresponding collection (and processing) of personal data is triggered by the filing of a complaint by (an) data subject(s) covered by Article 1 Service Regulations to the DPB in accordance with the Implementing Rules for Articles 1b and 32a of the Service Regulations ('Data Protection Rules' or 'DPR').

The Secretariat of the DPB registers the complaint and notifies the controller and the Chair of the DPB of the complaint. The Secretariat of the DPB informs PD08 and communicates the deadline for submission on considerations regarding the complaint.

For the PD08 Lawyers to prepare the controller's defence and prepare the submissions to the DPB, personal data stored on the complaint file is processed. The data is stored electronically.

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

Depending on the case, other business units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, may be involved in the fulfilment of certain supplementary tasks, such as execution of the DPB opinion and subsequent final decision.

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 DPB.

Upon receipt of a reasoned opinion from the DPB, PD 08 Lawyers process the DPB opinion and prepare a Note to the competent authority explaining the facts of the case, the DPB opinion and the recommended Final Decision. Such Note is shared with the competent authority together with the DPB opinion and the recommended Final Decision to enable them to make an informed, fair and balanced decision. Once the Final Decision is issued, the Secretariat of the DPB receives a copy of the Final Decision via email.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member initiates a complaint before the DPB.

The data collected may also be used for other purposes by the PD08 as e.g. to compile statistics and/or lists and carry out legal analysis for the hierarchy or other business units.

The processing of personal data is necessary in order to address all aspects related to the complaint file, 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 the DPB complaints and representing the controller's position for assessment by the DPB, concluding the DPB complaint procedure and issuing a final decision in accordance with Article 50(4) DPR and the creation of statistics and legal analysis, if necessary.

Personal data are processed for the following purposes:

- The fulfilment of the complaint procedure before the DPB.
- Providing PD08 with an understanding of the complainant's grievance and the surrounding circumstances.
- Establishing all of the facts to provide comprehensive submissions to the DPB on the controller's behalf.
- Providing the DPB with adequate information to enable the DPB members to deliver a reasoned opinion.
- Identifying cases that may be suitable for amicable settlement.
- Providing the hierarchy / competent authority with adequate information on the case to enable them to make an informed, fair and balanced decision.
- Issuing and where required, executing the Final Decision.
- Contacting the complainant(s) and notifying them of the Final Decision.
- Identifying recurring and systemic legal issues.
- On request, the preparation of statistics 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' using.

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) Complainant(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, employment status (active/inactive/retiree), professional contact details.
   - Litigation history (re past and pending disputes) if relevant for the case.
   - Any statements relating to the case.

- On a strictly need-to-know basis, any other categories of personal data provided by data subject or the respective delegated controller regarding themselves or in the context of information exchanged in submissions, concerning to the subject matter of the case, such as description of allegations, concerns, circumstances, description of facts, assessments, etc.
- Depending on the subject matter of the complaint, it might require the processing of special categories of data or of sensitive data.
  Such processing takes place on a strict need-to-know basis, only as necessary for the adjudication of the case.

(ii) Complainant's legal representative / successor(s):

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:

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

(iv) The external lawyer drafting submissions and representing the controller in front of the DPB:

Personal data may be processed such as:

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

(v) Individuals mentioned in the submissions:

Personal data may be processed such as:

- Identification details: name, surname.
- Any information related to them in the submissions.
- Their own statement, which can be required by the controller.

(vi) Witnesses/experts:

Personal data may be processed such as:

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

(vii) Employment Law Secretariat:

Personal data may be processed such as:

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

(viii) Data Protection Board Secretariat:

Personal data may be processed such as:

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

(ix) Members of the Data Protection Board:

Personal data may be processed such as:

- Identification details: name, surname (signature) of the members.

- Correspondence as well as their requests, opinions, procedural decisions.

(x) Competent Authority taking the final decision:

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 Data Protection Board, the competent authority taking the decision, the Data Protection Office and other internal operational units, 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 during the fact-finding exercise for complaints before the DPB.
(ii) The facilitation of comprehensive drafting of submissions to the DPB.
(iii) The execution of the Final Decision and the reassessment of a case by the relevant unit depending on the DPB opinion.
(iv) The preparation and use of statistics and lists.

External contractors involved in providing a platform and/or maintaining certain services such as Microsoft (Office, Exchange, Outlook, Teams), OpenText and Thomson Reuters (MatterSphere) and external lawyer representing the controller in front of the DPB 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 Data Protection Board and the Data Protection Board Secretariat.
b. The complainant’s legal representative where they are engaged in the procedure.
c. External lawyer representing the controller before the Data Protection Board.
d. 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 during the fact-finding exercise for complaints before the DPB.
(ii) The facilitation of comprehensive drafting of submissions to the DPB.
(iii) The execution of the Final Decision and the reassessment of a case by the relevant unit depending on the DPB opinion.
(iv) The preparation and use 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 complaint 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 Office's management and functioning.

Processing is necessary for the performance of the legal redress mechanism as foreseen by the Article 50 DPR and Rules of Procedure of the Data Protection Board.

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 complaint procedure will be stored until the last day of the 10th calendar year after closure of the case.

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.