

Data protection statement on the processing of personal data in the handling of Disciplinary Proceedings

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.

Initiation of proceedings before the Disciplinary Committee:

The appointing authority's involvement in the disciplinary procedure and the corresponding collection (and processing) of personal data is triggered when the appointing authority becomes aware of evidence or indications of misconduct. The appointing authority will determine whether the Disciplinary Committee must be convened.

Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers prepare a report which is then given on behalf of the appointing authority to the Disciplinary Committee. This report is also shared with the person concerned and their (legal) representative, if any.

The person concerned may also prepare submissions for the Disciplinary Committee. Submissions are made available to the concerned parties, the Disciplinary Committee and the PD08 Lawyer involved. The submissions are sent via email and stored electronically (subject to restricted access). All submissions are provided before a confidential hearing takes place. The hearing is attended by the person concerned, their (legal) representative, the Disciplinary Committee, witnesses and a PD08 Lawyer.

The Disciplinary Committee processes the submissions to prepare a reasoned opinion.

The Disciplinary Committee issues a reasoned opinion which is then shared with the person concerned and their (legal) representative, the appointing authority and PD08 Lawyers. PD08 Lawyers process the opinion and draft a note to the appointing authority containing legal advice on the Decision. The appointing authority processes the legal input and the Disciplinary Committee opinion when making an informed decision. The person concerned is heard by the appointing authority before the issuance of an informed decision. A Decision is signed by the appointing authority and sent by the secretariat in charge to the person concerned and their (legal) representative via email.

Disciplinary Proceedings before the competent authority:

The competent authority's involvement in the disciplinary procedure and the corresponding collection (and processing) of personal data is triggered when the appointing authority becomes aware of evidence or indications of misconduct. The appointing authority may decide to conduct disciplinary proceedings but not to convene the Disciplinary Committee depending on the seriousness of the allegations.

PD08 Lawyers process the DEC report to create a letter on behalf of the competent authority. This letter is shared with the appointing authority, the person concerned and their (legal) representative, if any. Electronic submissions are exchanged and sent via email. The correspondences are sent to the person concerned and

their (legal) representative, and received by the competent authority then shared with PD08. Files are stored electronically and are subject to restricted access.

Before the decision is taken, the person concerned is given the opportunity to state their case, orally or in writing. The competent authority may hold a confidential meeting attended by the person concerned, their (legal) representative, witnesses, if any and a PD08 Lawyer, depending on the case. Witness statements are also processed and stored electronically, subject to restricted access.

PD08 Lawyers process all submissions to provide legal advice to the competent authority on the Decision by means of a note to the hierarchy. The signed decision of the competent authority is sent by e-mail to the person concerned and their (legal) representative by the secretariat in charge.

General remarks applicable to both procedures

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 Disciplinary Committee.

The procedure may differ if a staff member involved in the decision making procedure concerning disciplinary procedure has a conflict of interest.

The entire disciplinary procedure is strictly confidential.

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

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

This data protection statement relates to the processing of personal data for the purpose of handling disciplinary proceedings as foreseen under Title VII Disciplinary Measures of the Service Regulations for permanent and other employees, the creation of statistics, lists and legal analysis, if necessary.

Personal data are processed for the following purposes:

- Provide the PD08 Lawyers with an understanding of the alleged misconduct of a person concerned and the surrounding circumstances, and to determine the possible sanction to be imposed.
- Allow PD08 Lawyers to prepare reports/submissions on behalf of the Office for the consideration of the Disciplinary Committee.
- Allow the person concerned a fair opportunity to defend themselves against sanctioning.
- Provide the Disciplinary Committee with adequate information to enable them to deliver a fair and balanced opinion.
- Prepare a Note to the appointing authority containing legal advice to make a reasoned Decision.
- Identify cases that may be suitable for amicable settlement prior to the case being fixed on the Disciplinary Committee's agenda.

- Prepare, statistics and legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time.
- Provide an archive of legal reference for PD08 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) The person concerned accused of misconduct:

Depending on the case and the need to prepare the Office's submissions and the Decision on the proceedings, various details about the person concerned are processed such as their:

- 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, employment status (active/inactive/retiree), engagement in additional tasks.
- 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 proceedings, it might require the processing of special categories of data or of sensitive data, such as:
 - o Health information
 - o Sex life or sexual orientation (especially in cases involving allegations of harassment or discrimination)
 - o Trade union membership
 - o Criminal offences, criminal convictions,
 - o History of previous disciplinary measures or sanctions against the person concerned.

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

(ii) Representative of the person concerned:

Personal data may be processed such as:

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

(iii) The witnesses / experts during a hearing and/or in the submissions:

Personal data may be processed such as:

- Identification details: name, surname, nationality (on a strictly need-to-know basis for the adjudication of the case).
- Professional details: Department, Grade and Step and role within the Office.
- History of previous dealings with the person concerned (disciplinary or otherwise).

(iv) 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 statements.

(v) PD 08 Lawyer:

Personal data may be processed such as:

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

- Legal statements or other communications.
- (vi) 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.
- (vii) The Disciplinary Committee Members:
 Personal data may be processed such as:
- Identification details: name and surname (signature).
 - Professional details: Title/Position and department within the EPO.
 - Correspondence as well as their requests, opinions, procedural decisions.
- (viii) Disciplinary Committee 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) The competent authority:
 Personal data may be processed such as:
- Identification details: name, surname (signature) of authority.
 - Professional details of the delegated data controller: professional email.
 - Correspondence and decision.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of 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 other internal operational units instrumental in the provision of information assisting in the investigation into the misconduct, the preparation of the decision on the proceedings and the execution of the sanction imposed referred to in this statement on a case-by-case basis, insofar as this is compatible with the principle of confidentiality.

External contractors involved in providing a platform and/or maintaining certain services such as Microsoft (Office, Exchange, Outlook, Teams), OpenText, Thomson Reuters (MatterSphere) and Cigna 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 Disciplinary Committee
- b. Secretariat of the Disciplinary Committee
- c. The concerned person's (legal) representative where they are engaged in the proceedings
- d. Witnesses/experts

Personal data are disclosed on a need-to-know basis to the EPO staff working in other internal operational units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, whose involvement is necessary and required by PD08 in the fulfilment of certain supplementary tasks such as:

- (i) the provision of information assisting in the investigation into the misconduct,
- (ii) the preparation of the decision on the proceedings and
- (iii) the execution of the sanction imposed referred to in this statement.

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

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 disciplinary 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 imposing of a disciplinary sanction in the event of proven misconduct by an employee as foreseen under Title VII Disciplinary Measures of the Service Regulations, Articles 93 and 94 of the ServRegs.

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 disciplinary proceedings 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 litigation, all data held at the time the litigation was initiated will be retained until the proceedings have been closed. Reference is made to the retention periods in litigation 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.