**Data protection statement on the processing of personal data in the handling of data in a Professional Incompetence 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.

**Referral of the case to the Joint Committee**

The competent authority's involvement in the professional incompetence procedure and the corresponding collection (and processing) of personal data is triggered by the President's decision to refer the case to the Joint Committee.

After three consecutive annual appraisals indicating unacceptable performance, the employee is offered the opportunity to remedy their lack of ability and efficiency. If the employee's performance does not improve, the Reporting Officer and the Counter-Signing Officer may escalate the case to the President. The case is processed by Principal Directorate Employment Law and Social Dialogue Advice (PD 08) Lawyers in order to advise the President on the seriousness of the case and whether to refer the case to the Joint Committee.

PD08 Lawyers process the evidence put forward by the Reporting Officer and Counter-signing Officer and prepare a reasoned proposal for appropriate measures on behalf of the President to the Joint Committee. The report from the appointing authority is also provided to the employee to which they are entitled to respond and request a complete copy of their personal file and all other documentation relevant to the proceedings. All files are prepared electronically.

The Joint Committee may order an inquiry in which they seek additional information. Both sides can make submissions and can respond to the submission of the other side. Witnesses may provide evidence during the proceedings.

The Joint Committee issues a signed reasoned opinion and transmits its reasoned opinion to the President and to the employee concerned.

PD08 Lawyers process the reasoned opinion and prepare a Note to the hierarchy outlining the appropriate sanction together with a recommended final decision. The final decision signed by the President is communicated to the employee concerned via email sent by the Employment Law Secretariat or the President's Office.

**Professional Incompetence Proceedings before the relevant authority**

The relevant authority's involvement in the incompetence procedure and the corresponding collection (and processing) of personal data is triggered by the President's decision not to refer the case to the Joint Committee. The relevant authority is entrusted to consider the case and to make a reasoned decision.

Following the employee's failure to remedy their lack of ability and efficiency, the Reporting Officer and Counter-Signing Officer may escalate the case to the President after three consecutive annual appraisal reports indicating unacceptable performance. This communication is done electronically. PD08 Lawyers process the evidence put forward by the Reporting Officer and Counter-signing Officer and prepare a reasoned proposal for appropriate measures for the relevant authority. The report from the appointing authority is also provided to the employee to which they are entitled to respond and request a complete copy of their personal file and all other documentation relevant to the proceedings. All files are prepared electronically.

PD08 Lawyers draft submissions on behalf of the Office. Any email correspondences are secured and sent and received by the Employment Law Secretariat. The relevant authority presides over an internal hearing attended by the employee. Witnesses may be heard, and witness statements processed and stored electronically on MatterSphere. The hearing is confidential.

PD08 Lawyers may provide the relevant authority with legal advice which is communicated in a Note together with a recommended final decision and sent by the Employment Law Secretariat via email. The final decision issued by the relevant authority is communicated to the employee concerned via email by the Employment Law Secretariat.

Depending on the case, other business units may be involved in the fulfilment of certain supplementary tasks, such as provision of information assisting in the examination into the unacceptable overall performance.

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 Joint Committee.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff is the employee concerned in the professional incompetence procedure.

The processing of personal data is necessary in order to address all aspects related to the consequences of the procedure, the creation of lists for archiving and monitoring of internal deadlines and legal analysis, if necessary.

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

This data protection statement relates to the processing of personnel data in a Professional Incompetence Procedure and for the creation of statistics and lists, and the legal analysis, if necessary.

Personal data are processed for the following purposes:

- Provide PD08 Lawyers with an understanding of the alleged professional incompetence and the surrounding circumstances, and to determine the possible sanction to be imposed.
- Allow PD08 Lawyers to prepare submissions on behalf of the Office for the consideration of the Joint Committee and the competent authority.

- Provide the Joint Committee with adequate information to enable them to deliver a fair and balanced opinion.
- Prepare a Note to the President 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 Joint Committee's agenda.
- Prepare legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time.
- Prepare statistics and lists for the hierarchy on request.
- 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 employee concerned:

The data provided by the requester is strictly necessary for the purpose. Depending on the case and the need for the legal advice, various details about the individuals may be processed such as:

- Identification details: name, surname, date of birth, nationality, marital status for the adjudication of the case. name, 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), performance history, depending on the case e.g. objectives, competencies, success criteria, probationary performance reports. Allowances received, rewarding history, remuneration.
- Litigation history (re past and pending disputes in relation with the proceeding at hand) if relevant for the examination.
- Any statements relating to the case.
- Depending on the subject matter of the proceeding, it might require the processing of special categories of data or of sensitive data, such as:
    - Health information.
    - History of any disciplinary measures or sanctions against the employee, if relevant for the examination.
    - Performance history (e.g. objectives, competencies, success criteria, previous appraisals, probationary reports).

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

(ii) Person assisting the employee concerned:

Personal data may be processed such as:

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

(iii) The witnesses giving a witness statement:

Depending on the circumstances of the case different parties may be asked to provide a witness statement such as the employee's line manager, their HRBP, or colleagues of the employee concerned. Various details may be collected and processed for this purpose 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.
- Decisions of previous legal/administrative proceedings with the accused employee, if relevant with the proceeding at hand.

(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.

(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 Joint 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, and recommendation.

(viii) 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 as well as decisions.

**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 competent authority taking the decision and internal operational units instrumental in supplementary tasks such as the provision of information or a witness statement, assisting in the examination into the unacceptable overall performance and the implementation of the administrative decision, 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) 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 Joint Committee
b. The person assisting the employee concerned where they are engaged in the proceedings
c. Witnesses/experts

Personal data are disclosed on a need-to-know basis to other internal operational units involved in the case or business units whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as the provision of information or a witness statement, assisting in the examination into the unacceptable overall performance and the implementation of the administrative decision taken, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality.

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).

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 professional incompetence 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?**

Processing is necessary 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 EPO or in the legitimate exercise of the official authority vested in the EPO.

Processing is necessary for the handing down of a sanction in the event of proven professional incompetence by an employee as foreseen under Article 52 ServRegs.

**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 professional incompetence proceedings will be stored until the last day of the 10th calendar year after closure of the case.

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.