Data protection statement on the processing of personal data in the context of the Legal Business Partner Brand in PD 5.2 Legal Affairs

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.

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

PD Legal Affairs serves as a centre of excellence for the provision of legal analysis, assistance and advice in legal matters with a strategic, policy, institutional or external dimension. We aim for a consistent delivery of legal service and ensuring the highest levels of quality and timeliness.

In this context, to provide senior management with a real-time overview of ongoing cases dealt with in Legal Affairs, PD52 makes a spreadsheet available to them with basic information on each case (such as lawyer(s) involved, subject matter) and associated legal risk evaluation.

This Case Overview is accessible to:

- Participating directorate's members who personally complete the information on their cases.
- Direct hierarchy up to the Vice-President DG5 and President of the Office, allowing earlier awareness and, if necessary, alignment. The prioritisation of cases based on associated risks serves as the primary indicator for senior management to discern where their attention may be most warranted.

Once a case closed, the corresponding entry is deleted from this list of ongoing cases. A list of closed cases with less data is kept separately in the same excel document, so that related information can be retrieved easily, should a question related to former cases come up later.

Personal data are processed for the following purposes:

- Defining and documenting roles and responsibilities
- Streamlining legal risk management
- Enhancing transparency towards stakeholders, ensuring that senior management is informed about which colleagues are responsible for specific cases; and
- Facilitating exchange and early alignment with Vice-President DG5 and/or the President of the Office in ongoing legal cases dealt with by Legal Affairs.

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

Your personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

2. What personal data do we process?

The following types/categories of direct identifiers are processed in the Case Overview:

- Name of case handler(s) and their deputy (for ongoing cases only; once a case is closed, these names are deleted).
- Information related to parties involved, such as names of units, company or individuals involved as internal stakeholders or external counsel.

Additionally, the Case Overview contains following types/categories of case-related data:

- Basic information on each case: Title/issue/project name, description of case, amount involved, status, important milestones.
- Risk assessment aspects such as risks involved, their likelihood, impact, rating, risk management actions.
- Associated case management references such as case management system ticket and/or clog references.

3. Who is responsible for processing the data?

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

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

Personal data is entered by Legal Affairs' case handlers who complete the information inserted by the assistants.

All members of the directorates concerned have access to the Case Overview, together with Principal Director PD 5.2, the DG5 Performance and Process Office, and Vice-President DG5. Access may also be granted to the President's Office.

External contractors involved in providing and maintaining platforms and tools necessary for the provision of services, such as Microsoft, may also access and process personal data.

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.

For systems hosted on EPO premises, the following basic security measures generally apply:

- user authentication and access control (e.g. role-based access to the systems and network, principles of need-to-know and least privilege)
- logical security hardening of systems, equipment and the network
- physical protection: EPO access controls, additional data centre access controls, 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 operates 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 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 that process the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks.

External providers are required to have implemented appropriate technical and organisational measures, such as:

- physical security measures, access and storage control measures, data security measures (e.g. 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 means of 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?

As a data subject, 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, please write to the delegated data controller via the Data Protection Officer, who is the point of contact for external data subjects, at DPOexternalusers@epo.org. EPO employees can contact PDLegalAffairs-DPL@epo.org. For us to respond 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 receiving it. 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 would inform you of any such delay.

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

Personal data are mainly processed on the basis of Article 5(a) DPR: 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, which includes the processing necessary for the EPO's management and functioning.

8. How long do we keep your data?

Personal data will only be kept only for the time needed to achieve the purposes for which it is processed.

The names of case handlers and deputies are only displayed as long as the associated case is ongoing. Further personal data remaining available on the list of closed cases (e.g. case management system ticket reference) is deleted at the latest two years after the end of the year in which the case was closed.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

9. Contact information

External data subjects who have any questions about the processing of their personal data should contact the delegated data controller via the Data Protection Officer at dpoexternalusers@epo.org. EPO staff can contact the delegated data controller directly at PDLegalAffairs-DPL@epo.org. They can also contact the Data Protection Officer at dpo@epo.org.

10. 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.