

## **Data protection statement on the processing of personal data within the framework of the Data Protection Board tasks, duties and activities**

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.

The EPO's Data Protection Board (DPB) is a statutory body established under Article 2(1)(h) and Article 32a(2) and (5) of the Service Regulations for permanent and other employees of the EPO (Service Regulations) and Articles 47 and 48 DPR. The DPB is composed of external experts, namely a chair, two members and one or two alternate members, and is supported by a secretariat made available by the EPO's Data Protection Office (DPO) to assist the DPB in its tasks, acting under the direction of the chair.

This data protection statement explains the way in which the DPB processes personal data to the extent necessary to carry out the tasks and duties assigned to it by the Service Regulations, the DPR, the [Rules of Procedure of the Data Protection Board](#) (RoP) and in compliance with additional operational documents governing the processing of personal data at the EPO.

The DPB fulfils a monitoring and advisory function within the legal redress mechanism under Article 50 DPR by receiving complaints from data subjects and by rendering reasoned opinions in their regard to the controller, who then takes the final decision on the data protection issue in question.

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

The DPB processes personal data in order to provide a reasoned opinion on complaints filed with the DPB by data subjects as part of the legal redress procedure under Article 50 DPR (hereafter: "complaint proceedings"). For more information on complaint proceedings, please refer to the [Rules of Procedure \(RoP\)](#).

In the context of complaint proceedings, personal data are processed for the following purposes:

- a. to register the complaint filed with the DPB using the appropriate [form](#) and to determine its receivability as provided for in Article 5 RoP
- b. to forward the complaint and any attached documents to the delegated controller responsible for the processing operation concerned, authorised parties involved in the defence of the EPO, the DPO and, where applicable, the processor in order for them to be informed of the complaint and prepare their submissions as applicable
- c. as the case may be, to facilitate an amicable settlement as described in Article 8 RoP; for more information on how your personal data are processed in the amicable settlement procedure, please refer to the relevant data protection statement
- d. to provide the DPB with adequate and sufficient information to enable it to render an opinion
- e. if required by the circumstances of the complaint, upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to co-operate with the competent national authorities, including competent national supervisory authorities or law enforcement authorities

- f. upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to share such data with a court or other judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body
- g. to share the reasoned opinion of the DPB with the controller and the parties involved in the procedure, including complainants, legal representatives (if any), delegated controllers and authorised parties involved in the defence of the EPO and the DPO
- h. to archive the opinion and the final decision of the controller, rendered after reception of DPB's reasoned opinion on SharePoint 2019 and MatterSphere

To carry out its tasks the DPB may request to access additional documentation (including legal, logistical and administrative support) deemed necessary, which may contain personal data.

Personal data contained in the opinions and related documentation received or sent by the DPB may be stored on the EPO's servers and/or in Microsoft Office cloud systems only accessible to authorised staff, namely:

- in Outlook in folders separated by year and/or on SharePoint 2019
- in the EPO document management tool (MatterSphere) with a specific number assigned to them

Redacted abstracts from the final decisions of the controller and the opinions of the DPB in the context of complaint proceedings may be published by the secretariat of the DPB on the EPO intranet and/or externally and be made available to all staff and the general public.

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

## **2. What personal data do we process?**

The following categories of personal data of the complainant and, if applicable, their legal representative may be processed in the context of complaint proceedings:

- name and surname
- email address
- if applicable, EPO username
- where applicable, physical location
- where applicable, telephone number, physical address and name of the company (only for the legal representative)
- signature
- any other categories of personal data (including special categories of personal data) provided directly by data subjects regarding themselves or received from third parties in the context of the complaint proceedings. Personal data may include the description of concerns, personal cases, circumstances, description of facts, evidence or arguments, opinions, assessments etc. Processing of special categories of personal data is on a strict need-to-know basis, and only as necessary for the DPB to carry out its tasks and duties.

Where possible, the DPB will refrain from processing special categories of data. However, should the occasion arise, appropriate technical and organisational security measures will be implemented to ensure the confidentiality and adequate protection of such personal data and minimise the possible risks for individuals.

In the performance of the tasks and duties assigned to it, the DPB may access additional documents, which may contain personal data relating to third parties (staff members or externals).

## **3. Who is responsible for processing the data?**

Personal data are processed under the responsibility of Principal Directorate 0.1 Chief of Staff, acting as the EPO's delegated data controller. The delegated controller shall adopt the technical and organisational measures necessary to guarantee the protection of the processed personal data, while the DPB remains autonomous and independent in the performance of its tasks in accordance with Article 48(6) DPR and Article 1(1) RoP.

Personal data are processed by the secretariat of the DPB in order to assist the chair, members and alternate members in carrying out the tasks and duties of the DPB referred to in this statement. Furthermore, the DPO may process personal data when acting upon request of the DPB in accordance with the tasks and responsibilities established under the DPR.

External contractors involved in Microsoft and MatterSphere may also process personal data for maintenance and support purposes, which will be always limited to accessing such data.

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

Personal data may be disclosed to the chair, members, alternate members and the secretariat of the DPB on a need-to-know basis and only to the extent necessary for them to carry out tasks and duties of the DPB. Additionally, personal data are disclosed to the recipients mentioned below.

Personal data may be disclosed on a need-to-know basis:

- to parties involved in the procedure, including complainants, legal representatives (if any), delegated controllers, the controller, authorised parties involved in the defence of the EPO and, where applicable, the processors, as well as to the DPO
- to the DPO and other parties that may be invited as observers during meetings of the DPB regarding the complaint
- to competent national authorities, including competent national supervisory authorities or law enforcement authorities acting within the scope of their respective competences if required by the circumstances of the complaint
- to a court or other judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body
- to other authorised EPO staff only to the extent necessary for them to handle the complaint

To this extent, personal data may be stored in one or more document management tools used by the DPB to perform its tasks, more specifically in MatterSphere, Microsoft Outlook and SharePoint 2019. Personal data will be stored and made available in these applications strictly on a need-to-know basis and for no longer than needed to achieve the purposes for which they are processed. For more information regarding the processing of personal data by these tools, please refer to the specific data protection statements.

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, IT security and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, 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 apply:

- user authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege)

- logical security hardening of systems, equipment and network
- physical protection: EPO access controls, additional access controls to datacentre, 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

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 stemming from the applicable data protection legal framework. The EPO has also carried out a privacy and security risk assessment.

These systems are required to have implemented appropriate technical, IT security 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 factual data processed in the context of the DPB's tasks, duties and activities.

If you would like to exercise any of these rights, please write to the [delegated controller](#), Principal Directorate 0.1 Chief of Staff, at [DPOexternalusers@epo.org](mailto:DPOexternalusers@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.

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

Personal data are processed in accordance with 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 Office's management and functioning.

In the framework of fulfilling their duties and tasks, the chair, members, alternate members and secretariat of the DPB may gather and manage special categories of data, such as health data, data related to the evaluation of performance and conduct etc. For such processing, Article 11(2)(f) applies in addition to Article 5(a) DPR. Personal data relating to criminal convictions and offences may be processed subject to the provisions of Article 12(1) DPR.

Furthermore, personal data are collected and processed in accordance with the following legal or operational instruments:

- [Rules of Procedure of the Data Protection Board](#)

- [Decision of the President of the European Patent Office identifying the operational units of the Office acting as delegated controllers](#)
- [Decision of the President of the Boards of Appeal appointing a delegated controller](#)

## **8. How long do we keep your data?**

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

Personal data related to complaint proceedings under Article 50 DPR will be stored in document management tools for a maximum of ten years after the complaint is withdrawn, found irreceivable or definitively resolved through a final decision taken by the controller which has not been challenged, an award issued in dispute resolution proceedings under Articles 50(8) and 52 DPR or an amicable settlement.

Members of the DPB shall destroy and/or erase any files or copies of files pertaining to a complaint case file within six months of the issue of the DPB's opinion.

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**

If you have any questions about the processing of your personal data, please write to the delegated data controller and/or our Data Protection Officer at [DPOexternalusers@epo.org](mailto: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 delegated controller under Article 49 DPR and, if you disagree with the outcome of the review, the right to ask the President of the Office to take a final decision. If you are dissatisfied with the controller's final decision you may seek legal redress under Articles 50(8) and 52 DPR.