Data protection statement on the processing of personal data in the framework of the Data Protection Office's 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.

This data protection statement explains the way in which the EPO's Data Protection Office (DPO) processes personal data in order to carry out the tasks and duties assigned to it by the Service Regulations for permanent and other employees of the EPO (Service Regulations), the DPR, other rules, administrative instructions and decisions adopted by the EPO President and additional operational documents governing the processing of personal data at the EPO.

The DPO may manage and assist other EPO delegated controllers in responding to data subjects' enquiries. Enquiries may be received either via the dedicated mailbox DPOexternalusers@epo.org or via other means (by direct contact with the EPO President or any delegated controller); in the latter case, the recipient will forward the enquiry to the said mailbox. Once an enquiry is received, authorised DPO staff will send an acknowledgement of receipt (from the dedicated mailbox) to the data subject and, where necessary, forward the enquiry to the relevant delegated controller, who will process and respond to it, in co-operation with the DPO. For consistency purposes, the final response will always be forwarded to the DPO together with any additional documents provided with it.

Additionally, the DPO maintains the Data Protection Register. The only personal data processed in this context are the cookies used on the EPO website. For more information on how cookies are managed, please refer to the relevant section in the Data protection and privacy notice.

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

The EPO DPO processes personal data in order to carry out the tasks and duties assigned to it, which include:

- managing data subjects' enquiries (meaning queries, requests to exercise data subject rights and requests for review by the delegated controller, complaints of alleged infringement of the DPR, including reports on potential personal data breaches) and assisting delegated controllers in responding to such enquiries
- managing the Data Protection Liaisons (DPLs) network (DPLs are the delegated controllers' contact points in relation to data protection matters)
- assessing risks for individuals resulting from personal data breaches
- carrying out data protection investigations and audits
- offering support to the Data Protection Board in carrying out its function under the DPR
- co-operating with other organs of the European Patent Organisation (i.e. the Administrative Council), European Union institutions, bodies, offices and agencies and/or other international organisations
- raising awareness/providing training on data protection matters

Personal data may be stored on the EPO's servers and/or in Microsoft Office cloud systems:

- all data subject enquiries, DPO opinions, advice and recommendations and related communications (together with supplementary documentation, as the case may be) received or sent by the DPO are stored in Outlook in folders separated by year and/or on SharePoint 2019 and are only accessible to

authorised staff. They are afterwards archived in the EPO document management tool (MatterSphere) with a unique identifier assigned to them
- where necessary, documents (e.g. drafts of operational documents, awareness-raising materials) may also be stored on SharePoint 2019

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

2. What personal data do we process?

The following categories of data subject personal data are processed:

- name and surname
- email address
- possibly physical address (together with country of residence)
- possibly legal representative's contact information (name, surname, email address, telephone number) and physical address
- telephone number
- any other categories of personal data (including special categories of personal data) provided by data subjects regarding themselves or in the context of information exchanged, such as company, organisational entity, description of concerns, personal case, circumstances, description of facts, opinions, assessments, etc. Personal data provided by data subjects may also concern subject-matter-related third parties

To carry out data protection investigations resulting from data subjects' enquiries, the DPO may process their personal data, such as contact information (name, surname and email address), and any personal data (related to them or third parties) included in the documentation provided to the DPO, which is necessary for the performance of the investigation. The enquirer's personal data contained in the final investigation analysis will be anonymised to the extent possible before it is shared with any internal stakeholders who were not involved in the investigation (such as the EPO President).

To carry out data protection audits, the DPO may access (on a strictly need-to-know basis) data subject personal data contained in the documentation provided to the DPO, which is necessary to carry out the audit. Personal data will only be processed for the performance of the audit.

When requested by the Data Protection Board (DPB) to provide support, the DPO may process, on a strictly need-to-know basis, personal data such as the details of the data subject filing a complaint, personal data contained in the allegations, and other categories of personal data depending on the case. For more information on the processing of personal data by the DPB, please refer to the relevant data protection statement.

Moreover, in the context of co-operation activities the contact details of external stakeholders (such as name and surname, email address, country of residence, possibly physical address and telephone number), their statements/opinions and any other related information may be processed.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Director Data Protection Office, acting as the EPO's delegated data controller.

Personal data are processed by the DPO's staff to carry out the tasks and duties assigned to the DPO, and potentially by the relevant delegated controller's DPL(s) (taking into account the case concerned and its sensitivity).

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 DPO, to the DPLs and to any other authorised EPO staff. To this extent, personal data may be stored in one or more document management tools used by the DPO to perform its tasks: MatterSphere, Microsoft Outlook, SharePoint 2019 and/or OpenText. 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.

Depending on the case, personal data may be disclosed to different recipients as follows:

- in the case of data subject enquiries, personal data may be disclosed to the delegated controllers responsible for the processing operation related to the enquiry. Strictly necessary personal data may be shared with other staff members (such as a technical team or human resources) as necessary to collect and compile relevant information to respond to the enquiry
- in the case of personal data breaches, personal data may be disclosed to the EPO President, the delegated controller, the processor and authorised staff as necessary to handle the breach
- in the case of an investigation under Article 43(1)(d) and (2) DPR, personal data may be disclosed to the person who commissioned the data protection investigation or the EPO President, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation
- in the case of an opinion requested from the DPO under Article 49(2) DPR, personal data may be disclosed to the delegated controller who received the request for review
- in the case of an opinion requested from the DPO under Article 51 DPR (these requests concern only former employees), personal data may be disclosed to the body under the Service Regulations advising the appointing authority and to the appointing authority

Personal data may be disclosed to the DPB when the DPO's support is requested.

In the context of co-operation with external stakeholders, personal data may be disclosed to authorised staff members of the DPO, the EPO President or the relevant delegated controller.

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 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 factual data processed in the context of the DPO's tasks, duties and activities.

In accordance with the DPR, restrictions to data subjects' rights based on Article 25(1)(c), (g) and (h) DPR, and Circular No. 420 implementing Article 25 DPR, may be applied in the context of the investigations and audits carried out by the Data Protection Officer in line with Article 43(1)(d) and (2) DPR.

If you would like to exercise any of these rights, please write to the delegated controller, the Director Data Protection Office, at 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 is 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.

The processing is necessary for the management and functioning of the EPO.

In the framework of fulfilling their duties and tasks, the DPO's staff members 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) DPR applies.

Furthermore, personal data are collected and processed in accordance with specific legal and operational instruments (e.g. the decision of the President of the European Patent Office identifying the operational units of the Office acting as delegated controllers).

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 related to co-operation with external stakeholders and related communications will be stored in the document management tool(s) for a maximum of 5 years after the closure of the case.

Personal data related to data subject enquiries will be stored in the document management tool(s) for a maximum of 10 years after the closure of the enquiry.

Personal data related to data protection investigations will be stored in the document management tool(s) for 10 years after the closure of an investigation.

Where a data subject's personal data are contained in the documentation provided to the DPO when it carries out data protection audits, personal data will be stored in the document management tool(s) for 5 years after finalisation of the final audit report.

Personal data related to the assessment of personal data breaches are stored for 10 years after finalisation of the data breach report.

Personal data processed to provide support and/or opinions or recommendations in relation to Article 49 DPR (request for review by the delegated controller), Article 50 DPR (legal redress) and Article 51 DPR (incidental data protection request during internal appeal proceedings – only relevant for former employees) will be stored in the document management tool(s) for 10 years after finalisation of the opinion.

The retention period of the personal data contained in the documents received by the DPO, in the performance of its tasks, is also defined in the records of operational processes supported by those documents.

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 at DPOexternalusers@epo.org.

You can also contact the Data Protection Officer at dpo@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.