Data protection statement on the processing of personal data as part of Customer Service Management

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 your personal data is handled as part of Customer Service Management.

When an enquiry is received at the EPO, the sender data are compared against the contact details in our database to identify the sender and allow their enquiry to be routed. This makes it possible to automatically acknowledge receipt of the enquiry, update and reply to the user and monitor any pending requests, in order to provide the best possible user experience. The contact details are only needed, processed and stored in so far as they are required to handle user enquiries about EPO tools, pending applications for a European patent, international PCT applications, opposition and limitation/revocation files, patent information issues and EPO products and to handle user questions, payment-related queries and other issues which are linked to the mission and services provided by the EPO.

Your anonymised data may also be used for statistical purposes and trend monitoring, as well as to gather information about categories of users or the types of issues users address.

All enquiries received are stored in the external processor's data centres located in Düsseldorf and Frankfurt, Germany.

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

Your personal data are processed in order to:

- respond to enquiries/questions/issues received as part of Customer Service Management
- gather information about categories of user or the types of issue users address (statistical purposes and trend monitoring)

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

The personal data processed as part of Customer Service Management are stored in Germany, which is considered a country where an adequate level of protection of personal data is ensured. Stored personal data are not accessed from a country that does not ensure an adequate level of data protection. Specific safeguards, including a data processing agreement with the provider, have been put in place to mitigate the risks.

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).

If the enquiries/questions/issues received relate to formal complaints or feedback, please refer to the data protection statement on the processing of personal data within the context of formal complaints and feedback.

2. What personal data do we process?

The categories of personal data processed are as follows:

- full name
- role/responsibility
- company name/organisation
- address
- contact details - (mobile) phone number, email address
- technical details (smart card number, epoline ID, preferred language)
- statements and opinions expressed when giving feedback on our services
- attendance at EPO events (visits, conferences, training)
- any other categories of personal data provided by the enquirer regarding themself or information exchanged, such as description of concerns, personal case, circumstances, description of facts, opinions, assessments, etc.

The ticket itself consists of the following elements:

- ticket number
- date
- description of the issue/question/problem reported/asked by the customer
- type
- priority
- assignee (team/person)
- activities (finding/solution/reply text)

The following types/categories of personal data may be processed regarding EPO internal employees and external EPO contractors who are involved in resolving customer service cases and related activities:

- full name
- telephone extension
- mobile phone number
- user ID
- email address
- office number and location

The above personal data may also be used for secure user authentication.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Principle Director 1.5 Customer Journey and Key Account Management, 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 Principle Directorate 1.5 Customer Journey and Key Account Management.

External contractors involved in providing and maintaining Customer Service Management software 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:

- DG 1: departments responsible for operations and quality management
- DG 4: Finance
- DG 5: Patent Law and the Legal Division

Personal data may be disclosed to third-party service providers for maintenance and support purposes.

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.

Additionally, in line with the requirements set forth in Article 6, limited access to personal data may be granted on a need-to-know basis should this be deemed necessary and proportionate for a specific purpose to EPO staff working in other organisational unit(s) to perform tasks carried out in the exercise of their official activities, e.g. so staff in D432 can prepare anonymised reports/analyses. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and the principles of confidentiality and accountability.

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 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

In principle, the EPO has adopted 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 a restricted access.

For personal data processed and stored in Customer Service Management software, the EPO has carried out a privacy and security risk assessment. The provider processing the personal data has committed in a binding agreement to comply with its data protection obligations stemming from the applicable data protection legal framework.

The provider's security framework is based on ISO/IEC 27002:2013. It has been an ISO 27001-certified organisation since 2012 and is also ISO/IEC 27017:2015- and 27018:2019-certified. The provider applies industry-recognised information security frameworks. These include ISO/IEC 27001:2013 and ISO/IEC 27017:2015 and 27018:2014, as well as accreditation with regional standards and regulations.

The software is required to have implemented appropriate technical and organisational measures such as:

- physical security measures
- access control measures: role-based, principles of need-to-know and least privilege
- storage control measures: access control, e.g. role-based, principles of need-to-know and least privilege
- securing data at rest, e.g. by encryption, secure disposal of data carriers
- user control measures: network security measures, e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), host security measures, e.g. antivirus, antimalware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, system hardening, vulnerability and patch management
- securing data at rest (e.g. by encryption)
- transmission control measures: audit logging, system and network monitoring
- input control measures: audit logging, system monitoring

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 can only apply to inaccurate or incomplete objective and factual data processed as part of Customer Service Management and does not apply to subjective statements.

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 as part of 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 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.

Your data can also be erased upon request.

Please bear in mind that data protection is not an absolute right. It must always be balanced against other fundamental rights and freedoms and there may be circumstances where one or more of a data subject's rights may be refused.

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 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 Office's management and functioning.

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. They will be stored as long as processing is operational.

Contact details will be stored for five years after they were last used or updated, i.e. after the last interaction with the data subject as part of Customer Service Management.

Personal data received with an enquiry will be anonymised five years after the ticket was closed, so it can be used for statistical purposes.

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 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.