Data protection statement on the processing of personal data in the context of the EPO Mail Service

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?

This data protection statement relates to the processing of personal data which takes place whenever EPO statutory, social and other bodies or employees request to use the EPO Mail Service.

Based on approved business cases (e.g. site-specific emails), which are established on business unit level, EPO statutory, social and other bodies or employees have the possibility to request Principal Directorate Communication (“PD Communication” or “PD0.2”) to use the EPO Mail Service to address internal and/or external data subjects.

To make use of the EPO Mail Service, Business units and employees need to request PD0.2 to direct their messages to all EPO employees or to a limited group of data subjects. To do so, the employees and the business units must indicate the desired recipients (e.g.: DD-ALL-STAFF) and the content of the message in the communication request form available on intranet for PD Communication approval and processing. Said requests are stored in a dedicated register owned by PD Communication for accountability purposes.

Once approved, the messages are sent to the designated recipients via the EPO Mail Service account.

The employees and the business units sending the emails remain responsible for the contents of their messages, including responsibility for any personal data potentially included in their messages.

Personal data are processed for the following purpose: managing the EPO Mail Service and giving the other EPO business units the possibility to send emails to designated data subjects.

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 categories of personal data may be processed:

- Contact details
  - Title (Mr/Ms/Other)
  - First name and last name

- Email address (professional or personal)
- Country of residence
- Job Title

- Office location
- User ID
- IP address

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of PD Communication, acting as the EPO's delegated data controller.

External contractors involved in the provision or maintenance of the EPO Mail Service 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 PD Communication, Business Information Technology (for support and maintenance purposes) and Principal Directorate People (as they are responsible for the directory of staff linked to the various distribution mailing lists).

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.

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 data centre, 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 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).

If you would like to exercise any of these rights, please write to the delegated data controller at PDComm-DPL@epo.org (internal) or DPOexternalusers@epo.org (external). 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 (internals) or this form (externals).

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) of the DPR, which states that “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 automatically deleted from the EPO Mail Service upon departure of the EPO employee from the Office , or upon request of the data subject to the relevant unit, if applicable.

Personal data stored in the PD Communication’s dedicated request register are deleted after 3 years upon receipt of the request.

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 PDComm-DPL@epo.org.

External users can refer to DPOexternalusers@epo.org, for their request to be processed.

You can also contact our 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.