Data protection statement on processing personal data for the EPO Contingency Upload Service for parties to proceedings before the EPO

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 Contingency Upload Service is a tool to be used in exceptional cases where the standard filing solutions are not available. It enables users to upload one or more documents and receive a confirmation from the EPO that they have been received and stored securely, together with the timestamp for this receipt.

1. What is the nature and purpose of processing?

This data protection statement relates to the processing of personal data for the purposes of the EPO Contingency Upload Service when uploading documents for patent-grant and related proceedings (PGP) pursuant to the EPC and the provisions applicable under it, and likewise proceedings under the Patent Cooperation Treaty (PCT) and the Unitary Patent Rules (UPR).

Personal data are collected when users upload one or more documents via the EPO Contingency Upload Service. Uploaded data are encrypted and stored securely on infrastructure operated by the EPO and hosted on the EPO's cloud service provider (Google Cloud Platform).

Personal data are used to identify the user performing an upload and/or any other party signing the uploaded package. Submissions are frequently signed by a different person from the one logged into the system. As part of each upload in the EPO Contingency Upload Service we therefore ask the user to fill in information about the signing party and provide a text string signature matching the signing party's name.

Personal data are also processed using the PGP back office systems that allow EPO staff to process patent applications and any other subsequently filed documents pursuant to the EPC, the PCT, the UPR and the provisions applicable under them.

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 categories of personal data are processed as part of the information the user is asked to provide for each upload:

- Contact information:
    - First name
    - Last name
    - Email address
    - Telephone number (mobile or other phone numbers)
    - Company or organisation
    - Address
- Signatory information:
    - Name of the signing party (first name, last name and other name(s) provided)
    - Function of the signing party
    - Place of signing
    - Text string signature

The following personal data may also be included within request forms or other documents attached with an upload:

- Contact details
- Country
- Home address
- Mobile and other phone numbers
- Work email address
- Company entity
- Department name and/or number
- Job title role
- Office location
- Address from European Patent Register
- Bank account information
- Credit card number
- Debit card number
- National ID card details
- Passport number
- Patent record bibliographic and meta data

These data are processed in line with the relevant provisions of the EPC, in particular:

- Applicant's name (i.e. family name and given names), address, nationality and state of residence or principal place of business (Rule 41(2)(c) EPC)
- Applicant's fax and telephone numbers and email address, where provided (Rule 41(2)(c) EPC)
- Applicant's signature (Rule 41(2)(h) EPC)
- Name of any representative, their signatures, the address of their place of business (Rules 143(1)(h), 41(2)(d), 92(2)(c) EPC) and, where provided, representative number, association number, fax and telephone numbers and email address
- Inventor's name and country and place of residence (Rule 19(1) EPC)
- Personal data contained in copies of previous applications where applicants claim their priority (Rule 53(1) EPC)
- Name of the person making a payment and personal data relating to deposit accounts or other means of payment (bank accounts, credit cards, etc.) (Article 6(1) RFees, Article 5(2) RFees together with the Arrangements for Deposit Accounts)
- Where applicable, any personal data relating to third-party observations, evidence, prior art, IT tools and services and oral proceedings
- Any other personal data provided by a party during the proceedings

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of DG 1's PD 15 Customer Journey and Key Account Management, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff in departments 1195 (Classification Support, File Management, SCAPES and CDR) and 45331 (Front Office Tools) responsible for operating the EPO Contingency Upload Service.

DG 4 staff and external contractors involved in maintaining the EPO Contingency Upload Service may also process or have access to personal data.

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

Personal data are processed by the departments of the EPO specified in Article 15(a) to (e) EPC. This includes EPO staff involved in:

- carrying out the procedures laid down in the EPC, the PCT and the UPR and the legal provisions applicable under them
- providing user and technical support
- improving the patent grant process and the EPO Contingency Upload Service.

Personal data are disclosed on a need-to-know basis to the EPO staff working in DG 1 Patent Granting Process, the Boards of Appeal Unit, DG 4 Business Information Technology and DG 5 Legal Affairs.

External contractors involved in providing, maintaining and offering support for the EPO Contingency Upload Service may also process personal data, which can include accessing them.

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 processed and stored in secure IT applications in accordance with the EPO's security standards. These include:

- user authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication
- access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege): administrative and user roles are separated, users have minimum privileges, overall administrative roles are reduced to a minimum
- logical security hardening of systems, equipment and network
- physical protection: EPO access controls, additional access controls to the 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

Appropriate levels of access are granted individually only to the recipients listed above. As a contingency service, the EPO Contingency Upload Service is hosted on the EPO’s cloud service provider (Google Cloud

Platform). This provider has committed in a binding agreement to comply with its data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. The provider's systems are required to implement appropriate technical and organisational measures. These include 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, a network intrusion detection system, network intrusion protection system, audit logging) and conveyance control measures (e.g. securing data in transit by encryption).

On top of the standard security measures implemented by the provider, the following has been specifically implemented for the EPO Contingency Upload Service:
The upload package (i.e. the documents included in an upload) is zipped and encrypted with the AES-256 algorithm. A different encryption key is generated for each package. The package is stored in encrypted form.

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).

As with all secondary legislation adopted by the Administrative Council in accordance with its powers under Article 33(2) EPC, the DPR are subject to the provisions of the EPC, including its Implementing Regulations, which form an integral part of the EPC under Article 164(1) EPC. In addition, where the EPO is acting as PCT receiving Office and International Authority, it is bound first by the PCT legal framework, which consists of the Patent Cooperation Treaty, its Regulations and the related secondary law, i.e. the Administrative Instructions, the Guidelines for receiving Offices and the International Searching and Preliminary Examination Guidelines. Accordingly, any data subject rights under the DPR apply only to the extent that they do not conflict with the provisions of the EPC and its Implementing Regulations and, where applicable, of the PCT legal framework.

The same applies *mutatis mutandis* to proceedings conducted under the UPR (Rules relating to Unitary Patent Protection) and the RFeesUPP (Rules relating to Fees for Unitary Patent Protection), including the provisions applicable under them, as set out in the annex of the Decision of the President of the European Patent Office dated 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect. In case of conflict, the provisions of the UPR and the RFeesUPP, including the provisions applicable under them, take precedence over the Data Protection Rules.

If you would like to exercise any of these rights, please write to the delegated data 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.

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 5a 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) and Article 5b DPR (processing is necessary for compliance with a legal obligation to which the controller is subject).

In particular, personal data are processed for the purposes of the EPO's task under Article 4(3) EPC of granting European patents, as further specified in the relevant provisions of the EPC and the other provisions applicable thereunder. Where these data are required for proceedings under the EPC, their processing is mandatory (mandatory personal data). The same applies *mutatis mutandis* to data required for proceedings under the PCT and the UPR.

For the processing of personal data in proceedings related to European patents with unitary effect, please see the Decision of the President of the European Patent Office dated 7 December 2022.

8. How long do we keep your data?

A patent provides legal protection for 20 years, and there is no limit on how long the post-grant procedures can last: after the patent granting procedure, there may be an opposition procedure which will review the patent granting procedure and involve members of the examining division. These members need to be able to retrieve their actions and comments. Following the patent granting procedure there can also be an appeal procedure, which may result in the examination procedure being reopened by the examining division. After that, revocation and limitation procedures may take place at any time, even after patent protection has expired. The examining division needs to be able to retrieve the actions and comments of the initial procedure. For more information, see the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98). Personal data used which are part of the patent grant procedure are stored indefinitely. If considered appropriate, other personal data (for example the names of administrative staff of a representative that process uploads performed via the EPO Contingency Upload Service) can be deleted after a maximum of 10 years if it can reasonably be expected that there is no operational need for them anymore. 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 the Data Protection Officer at DPOexternalusers@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.