Data protection statement on the processing of personal data in the context of the European Patent Administration Certification

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 personal data are processed for the administration and the conduct of the European Patent Administration Certification (hereafter EPAC) as defined in the Rules concerning the establishment of a European Patent Administration Certification (EPAC). This includes personal data of candidates and members of the EPAC bodies.

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

Personal data are processed by the EPO to successfully organise and manage the European Patent Administration Certification (such as to identify candidates, to accurately associate candidates' examination answers, to ensure that the examination is conducted properly as well as to prevent and prove attempts of fraudulent behaviour) and follow-up actions in accordance with the Rules concerning the establishment of a European Patent Administration Certification, hereafter referred to as EPAC Rules.

The present document aims at providing information on how the personal data are processed in the context of the different stages and activities of the EPAC, such as registration and enrolment of the candidates, the correct performance of the examination, the provision and publication of the result and the review requests as well as the selection and appointment of the EPAC Board and Review Board members.

The examination is organised and conducted by the EPO's Patent Academy by delegation of the President of the EPO. The composition and duties of the bodies as well as the procedures to appoints their members are regulated in the EPAC Rules. The names of the members are published online once they have been appointed by the President of the EPO.

Members of the EPAC Board and the EPAC Review Board provide their data when applying to become member of the respective body. The information is entered into the system by the EPO's Patent Academy.

According to Article 6 of the EPAC Rules, candidates intending to enrol for the EPAC must request their enrolment by means of the enrolment tool provided on the website of the EPO: documentation that proves their identity and which will enable the EPO's Patent Academy to take up contact with the candidates (such as email and postal addresses, phone numbers, gender, nationality).

Formal requirements are assessed by the EPO's Patent Academy, who decides on the enrolment of candidates in accordance with the EPAC Rules. The EPO's Patent Academy checks if the formal requirements are met and, in case of doubt, asks the provider of the data for further evidence.

These activities include the processing of personal data for the assessment of special cases (disabilities), for the candidates' enrolment as well as for the payment of the fees.
Candidates with disabilities are flagged in the system as needing special arrangement, the medical details of the disability as such are not named nor stored, since only compensation is offered. Correspondence with candidate is kept in his/her file as long as the candidate is active in the EPAC.

The examination results are made available by the EPO's Patent Academy to each candidate. According to Article 16 EPAC Rules, candidates' anonymity shall be respected when their answers are marked and their answers may be published for research, statistical or training purposes provided their anonymity is respected.

The external supplier providing the platform for the online EPAC, processes personal data on the EPO's behalf and it is in charge of the maintenance of the platform and the provision of support. The online platform has proctoring features to monitor the candidates during the examination so as to prevent – or provide evidence of- fraudulent behaviour where deemed necessary.

Personal data are processed for the following purposes:

- to identify candidates of the EPAC,
- to establish the fulfilment of conditions to enrol,
- to determine that relevant fees are paid,
- to grant access to the online exam platform,
- to accurately associate the examination answers to the candidates,
- to ensure that the examination is conducted properly (including technical support to the candidates by the EPO master users), and that attempts of fraudulent behaviour are prevented or proven,
- to anonymously assess the candidates' examination answers,
- to establish a pass or fail of a candidate,
- to process possible review requests
- to publish the list of successful candidates
- to administer the members of the EPAC bodies as defined under Article 3 EPAC Rules.

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.

Personal data are stored in the EU according to the application configuration implemented by the EPO. They may, however, be made available to the sub-contractor in the US for support services within the online platform. The external provider has in place the suitable safeguards (e.g., DPA, EU SCCs) to transfer personal data to recipients under Article 9 for such purposes support services.

2. What personal data do we process?

Personal data relates to:

- EPAC candidates
- members of the EPAC bodies as defined under Article 3 of the EPAC Rules who are either EPO employees or external members, and other specific EPO authorised users (master users).

The stored data for the EPAC candidates comprise:

- Identifying information: Names, birth date, place of birth, gender, nationality, copy of an identity card
- Contact Information: postal address, e-mail address, telephone number
- Language preferences
- Information on disabilities for candidates requesting special conditions: copies of certificates, flagging

in system

- Examination answers and results: result data, copies of documents, when appropriate review decisions
- Online Invigilation: Webcam captures, facial images, audio, biometric data produced from webcam and audio captures, IP address
- Other administrative data: language preferences, payment dates, mail exchange
- Content of the communication (chat) between the candidate and an invigilator, the EPO's Patent Academy, or other technical support staff during the examination
- Any other data which is required to implement the EPAC Rules.

Except for the payment dates, the system does not store individual financial data such as bank account numbers or credit card numbers.

The stored personal data for the EPAC bodies (EPAC Board and EPAC review Board) comprise names, gender, nationality, contact information, language preferences.

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the Principal Director Patent Intelligence, acting as delegated EPO data controller.

Personal data are processed by the EPO staff of the EPO's Patent Academy and the relevant members of the EPAC bodies (EPAC Board and EPAC review Board) involved in the administration and conduct of EPAC.

External contractors involved in the organisation of the EPAC may also access the personal data processed.

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

Personal data will only be shared with authorised persons responsible for the corresponding processing operations and are not used for any other purposes or disclosed to any other recipients. The personal data are disclosed on a need-to-know basis to the to the following recipients:

- the EPO's staff members of the EPO's Patent Academy;
- members of the EPAC Board and EPAC review Board;
- specific EPO authorised users (`master` users)
- administrators of the data processors UNIwise.

UNIWise might access to the following data from the EPO master users and the members of the EPO's Patent Academy for the purposes of the bidirectional communication channel (chat) during the examination:

- First name
- Surname
- Email address
- Preferred language
- IP address
- Content of the communication (chat) between the candidate and the EPO's Patent Academy member acting as invigilator.

The hosting service for the UNIWise processor is provided by AWS Amazon (Ireland).

Of the above-listed personal data, only facial images, audio and biometric data produced from webcams, and audio captures are processed by AWS Amazon for the purposes of the AI-based invigilation. The other data categories are merely hosted and stored in their system in an encrypted form.

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, alteration and unauthorised disclosure or access.

All personal data are stored in secure IT applications according to the EPO's security standards. Appropriate levels of access are granted individually only to the abovementioned 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.

The EPO has assigned respective access rights to make sure that the personal data is protected and that all possible measures have been taken to safeguard the confidentiality, integrity and availability of the information.

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. When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out and the following general statement might be included in this field:

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 data processors have restricted access and committed to comply themselves and ensure the compliance of their sub-processors with the data protection rules and requirements in specific data processing agreements.
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 PDPatentIntelligence-DPL@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, which states that 'processing is necessary for the performance of a task carried out in the legitimate interest of the official authority vested in the European Patent Office'.

Personal data is collected and processed in accordance with the following legal instrument: Decision of the President on Rules concerning the establishment of a European Patent Administration Certification (EPAC).

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.
The EPO is committed to good practice in records management, and in particular is committed to retaining information for as long as necessary and no longer. The retention periods for different types of documents is determined by consideration of the operational, legal and contractual requirements, and in line with best practice. The periods shall be counted from the final decision or latest action.

It applies to all documents and information obtained and produced in electronic and/or paper form in connection with a candidates' enrolment and participation in the EPAC.

Group of record	Retention period	Reason for length of period
Records documenting the admission of candidates	50 years	Good practice, avoid fraudulent behaviour
Records documenting the results of candidates	50 years	Good practice and proof of final award fulfilled)
Records of a candidate's participation	50 years	Basis for fee increment; financial accountability
Candidates' answer papers	10 years	Good practice
Records documenting the review procedure of candidates	10 years	Good practice

The personal data, which are exclusively processed for the conduct of the examination in the online format, will be deleted from the EPO, the data processor`s and sub-processors' systems in maximum 30 months after the examination, or the conclusion of review requests, if any exist in relation to the examination.

Facial images, audio and biometric data produced from webcam and audio captures will be deleted by the processor's and sub-processors' systems after 6 months from the examination.
In a case of suspected misconduct and/or review request, the data, which are mentioned above as being retained by the processor and the sub-processors for a short period, will be copied and retained by the EPO for the longer period up to 30 months, or up to the conclusion of the review request, if any exist in relation to the examination.

In the event of a review request, all data held at the time of the review request shall be retained until the completion of its process.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at the following email address: PDPatentIntelligence-DPL@epo.org

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 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.