

## **Data protection statement on the processing of personal data in the context of the European qualifying examination**

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 qualifying examination (hereafter EQE) as defined under Article 134 of the European Patent Convention (EPC). This includes personal data of candidates and members of the EQE bodies.

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

The EPO processes personal data in order to successfully organise and manage the European qualifying examination (e.g. to identify candidates and link them to their examination answers, to ensure that the examination is conducted properly and to prevent – or provide evidence for – attempts of fraudulent behaviour) and follow-up actions in accordance with Article 134 EPC and the Regulation on the European qualifying examination (REE) and its implementing provisions (IPREE).

The present document provides information on how the personal data are processed in the different stages and activities of the EQE, such as the registration and enrolment of the candidates, the correct performance of the examination, the provision and publication of the results and any appeals, and the selection and appointment of the committee members.

The examination is organised and conducted by a Supervisory Board, an Examination Board, Examination Committees and an Examination Secretariat. The composition and duties of these bodies and the procedures for appointing their members are regulated in the REE (Articles 2 to 10) and IPREE. The names of the members are published online once they have been appointed by the President.

Members of the Supervisory Board, Examination Board and Examination Committees provide their data when applying to become a member of the respective body. The Examination Secretariat enters the data into the system.

According to Rules 1 and 28 IPREE and Article 11 REE, candidates intending to enrol for the European qualifying examination for the first time must register once they have commenced their professional activity within the meaning of Article 11(2) REE. Candidates must upload all supporting documents (to prove their identity, academic qualifications and professional requirements) to the web portal. When required, paper documents are entered into the system by the Examination Secretariat.

Formal requirements are assessed by the Examination Secretariat, which decides on the registration and enrolment of candidates in accordance with the REE and the IPREE. The Examination Secretariat 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 registering the assessment of special cases (disabilities), the candidates' enrolment and payment of the fees. Candidates with disabilities are flagged in the system as needing special arrangements; the medical details of the disability as such are not named nor stored. Any correspondence with candidates is kept in their files as long as they are active in the EQE.

The answers are marked, and the results registered by the markers in the online portal and verified by the Examination Board. The Examination Secretariat offers candidates access to their results, including the marking sheets pertaining to their answer papers.

In accordance with Article 21 REE, candidates' anonymity will be respected when their answers are marked. The answers may be published for research, statistical or training purposes provided the candidates' anonymity is respected.

The appeal procedure before the Disciplinary Board of Appeal under Article 24 REE follows the rules of this Board and the additional Rules of Procedure of the Disciplinary Board of Appeal of the European Patent Office. The texts of these Rules, the business distribution schemes of the Boards and other information on the Boards and the appeals procedures are contained in an annual supplement to the EPO Official Journal entitled "Information from the Boards of Appeal".

The external supplier providing the platform for the online EQE processes personal data on the EPO's behalf and 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 European qualifying examination
- to establish the fulfilment of registration and enrolment conditions
- to determine that relevant fees have been paid
- to grant access to the e-exam platform
- to link the examination answers to the candidates
- to ensure that the examination is conducted properly (including technical support for candidates by EPO master users) and to prevent - or provide evidence of - fraudulent behaviour
- to anonymously assess the candidates' examination answers
- to establish a pass or fail of a candidate
- to process appeals
- to publish the list of successful candidates
- to enable the selection of Examination Committee members (Article 7 REE)
- to maintain records relating to the members of the EQE bodies as defined under Article 1(6) REE
- to obtain feedback by means of surveys

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 is required to implement appropriate safeguards (i.e. DPA, EU SCCs) for the transfer of personal data to recipients under Article 9 DPR for such purposes.

Data is additionally processed for the purpose of surveying participants for feedback, including from EQE candidates, relating to the examination experience including specific issues related to disabilities and specific conditions. Anonymised statistical analysis information may be shared with third parties.

## 2. What personal data do we process?

Personal data relate to:

- EQE candidates
- members of the EQE bodies as defined under Articles 1 (6), 2, 4, 7 and 9 REE (the Supervisory Board, the Examination Board, the Examination Committees and the Examination Secretariat respectively) who are either EPO employees or epi members, and other specific EPO authorised users (master users).

The personal data processed for EQE candidates comprise:

- identifying information: names, birth date, place of birth, gender, nationality, copy of an identity card
- contact information: postal address, email address, telephone number, fax number
- qualifications: documents certifying academic education and qualifications, types and dates of degree awards
- professional activity: certificate of training or employment indicating periods of professional activity signed by supervising professional representative or external firm. For EPO examiners, certificate indicating time spent as examiner
- information on disabilities for candidates requesting special arrangements: copies of certificates, flagging in system
- examination answers and results: result data, copies of documents, appeal decisions (if applicable)
- online invigilation: webcam captures, facial images, audio and biometric data produced from webcam and audio captures, IP address
- other administrative data: language preferences, payment dates, mail exchange
- content of communications (chat) between the candidate and an invigilator, the Examination Secretariat or technical support staff during the examination
- any other data required to implement the Regulation on the European qualifying examination (REE), its implementing provisions (IPREE) (Supplementary publication 2 – Official Journal EPO 2019) and any by-laws or instructions based on the REE or IPREE.
- Survey related information which might be provided in the course of exchanges or voluntarily
- Any other information in relation to surveys

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

The personal data stored for members of the EQE bodies (Examination Committees and the Examination Board) comprise names, gender, nationality, contact information, language preferences and relevant data relating to when they were EQE candidates themselves.

## 3. Who is responsible for processing the data?

Personal data are processed 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 Examination Secretariat and the relevant members of the EQE bodies (Examination Committees and the Examination Board involved in the administration and conduct of the EQE).

External contractors involved in the organisation of the EQE and surveys 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 following recipients:

- the EPO's staff members of the Examination Secretariat
- members of the Examination Committees and the Examination Board
- specific EPO authorised users ("master" users)
- administrators at the data processor, UNIwise

As sub-processors of UNIwise, Comm100 Network Corporation may access the following data from the EPO master users and Examination Committee members 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 Examination Committee member acting as invigilator

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

Of the personal data listed above, only facial images, audio and biometric data produced from webcams, and audio captures are processed by AWS Amazon for the purposes of 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 in accordance with the EPO's security standards. Appropriate levels of access are granted individually and 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 personal data are protected and that all possible measures have been taken to safeguard the confidentiality, integrity and availability of the information.

In principle, the EPO uses 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 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:

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 have committed

to comply 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. The systems not hosted on EPO premises 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) and 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 send an email to the delegated data controller at [PDPatentIntelligence-DPL@epo.org](mailto:PDPatentIntelligence-DPL@epo.org). In order to enable us to respond more promptly and precisely, you should always 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 receiving it. 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 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 are collected and processed in accordance with the following legal instrument: Article 134 EPC and the Regulation on the European qualifying examination ([Supplementary publication 2 – Official Journal EPO 2019](#)).

## **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 are determined by consideration of the operational, legal and contractual requirements, and in line with best practice. The periods are counted from the date of the final decision or latest action.

The retention periods are established in the 'Archiving and Retention policy for the European qualifying examination (EQE)' document - decision by the Supervisory Board of the EQE, which applies to all documents and information obtained and produced in electronic and/or paper form in connection with a candidate's registration, enrolment and participation in the EQE.

Category of records	Retention period	Reason for length of period
Records documenting the admission of candidates	50 years	Good practice, avoidance of fraudulent behaviour
Records documenting the results of candidates	50 years	Good practice and proof of final award (i.e. requirements of Article 134 EPC 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 appeal 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 processors' and sub-processors' systems no later than 30 months after the examination or the conclusion of appeal proceedings, if any exist in relation to the examination.

Facial images, audio and biometric data produced from webcams and audio captures will be deleted by the processor's and sub-processors' systems six months after the examination.

In cases of suspected misconduct and appeal cases, the data 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 a longer period of up to 30 months or, if applicable, until the completion of the appeal proceedings.

In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal proceedings.

## 9. Contact information

If you have any questions about the processing of your personal data, please send an email to the delegated data controller at the following address: [PDPatentIntelligence-DPL@epo.org](mailto:PDPatentIntelligence-DPL@epo.org).

You can also contact our Data Protection Officer at [dpo@epo.org](mailto: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 a review by the controller under Article 49 DPR. If you disagree with the outcome of the review, you have the right to seek legal redress under Article 50 DPR.