

Data Protection Statement on the processing of personal data in interpreting services

Protecting your privacy is of the utmost importance to the European Patent Office (EPO, or Office). 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 statement refers to the processing of personal data **in interpreting services**.

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

The personal data of the interpreters engaged by the EPO are processed for the purpose of providing the EPO with the services of interpreters of the highest standard of ability, efficiency and integrity.

To be eligible for work from the EPO, interpreters submit a bid to the EPO's Procurement department via the Dynamic Purchasing System (DPS). Candidates submitting a successful bid are awarded a framework contract or, depending on demand for their language combination, are placed on a waiting list for future consideration, where they may remain for up to five years.

Candidates awarded a contract first undergo an onboarding process, including e-learning, dummy booth practice and induction tests. Candidates passing these tests then enter a test phase where they receive paid assignments and feedback.

At the end of the test phase, the EPO decides whether to accredit an interpreter. Only accredited interpreters may continue working for the EPO. Decisions on accreditation are taken by EPO Language Services based on the feedback from the test phase.

Interpreters' personal data are stored and processed on OpenText and in the Interpreter Administration System (IAS).

To ensure interpreting services are of the required quality, interpreters receive feedback, particularly from the induction tests and during the test phase. The associated data are stored in a restricted email account within Language Services and in MS Forms.

Overall, the processing of personal data is necessary for:

- keeping a pool of accredited and appropriately qualified interpreters
- interpreting service provision
- quality management purposes (induction and assessment of new interpreters and ensuring service quality)
- administering the payment process

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 categories of personal data processed are as follows:

- personal data contained in bid documents: title, first and last name, address, professional domicile, address for tax purposes, phone number, mobile phone number, email address, bank details, working languages, education data, professional experience, CVs, degree certificates, mother tongue, VAT status and number, availability (when interpreters were (not) available, when they worked for the EPO) – these data are stored in IAS, function, **evidence** of relevant experience, company name, legal form and contact details of the head office, commercial register number
- feedback on service quality. Only performance-related data that is strictly necessary to onboard and assess new interpreters and to monitor service quality is collected and processed.

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of DG 4 - PD 44 – General Administration acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in interpreting services. Performance-related data are obtained as a result of evaluations performed by the quality management team of senior interpreters.

EPO-external technicians involved in organising oral proceedings with interpretation process limited personal data.

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

Interpreters' personal data are accessible to:

- the Language Services Director
- the Team Manager Interpreting
- the Interpreting and Central Support staff responsible for interpreting services

EPO-external technicians involved in the organisation of oral proceedings have limited access to interpreters' personal data to enable the oral proceedings.

Personal data will only be shared with authorised persons responsible for the corresponding processing operations; access to the performance-related data is restricted to a limited number of

authorised persons involved in interpreter quality management; and the data is not 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, alteration and unauthorised disclosure or access. EPO personal data are processed in secure IT applications according to the security standards of the EPO.

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): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum,
- Logical security hardening of systems, equipment and network: 802.1x for network.

IAS is a secure IT application according to the security standards of the EPO.

These include:

- User authentication: internal access (by Directorate Language Services) is based on Windows authentication, with Single Sign On, based on active directory groups. External access by interpreters is via IAS External. IAS External is defined as an Azure application (<https://onpremiseiasexternal-epocloud.msappproxy.net/>). Authentication is based on the Standard authentication method defined for all EPO Azure applications (Windows user account + password + Multiple-factor authentication),
- Access control: IAS and IAS External have only two roles: internal users or interpreters. These roles are “hard-coded” in the application and managed by Active directory groups. Requesters are not defined in the application: any EPO user can access the page for requesting interpreting services in IAS Internal
- Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk,
- Security incidence response: 24/7 monitoring for incidents, on-call security expert.

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 factual data processed in the context of the EPO’s tasks, duties and activities; it does not apply to subjective statements, including ones made by third parties. With regards to the right of access, where the EPO considers it necessary to protect the confidentiality of internal deliberations and decision-making, certain information may be deleted from the copy of personal data provided to the data subject.

Access to personal data is available at any time via IAS External. Any inaccuracies may be rectified by using the "UPDATE" button provided within the system.

For performance-related data, a copy of each performance report is provided. This enables review of the information and, where necessary, the correction of any factual errors may be requested.

If you would like to exercise any of these rights, external users should write to DPOexternalusers@epo.org, otherwise contact the delegated data controller at dpl.pd44@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](#) (for externals) or this [form](#) (for internals) 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 based on Article 5(a) and (b) DPR.

(aa) Processing is necessary for the management and functioning of the EPO

(b) Processing is necessary for compliance with a legal obligation to which the controller is subject.

Applicable legal instruments: Rule 4 EPC

8. How long do we keep your data?

Bids and contracts are subject to a retention period of 12 years.

All other data is subject to a retention period of 15 years.

In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

9. Contact information

If you have any questions about the processing of your personal data, externals should contact the DPO and/or the delegated data controller at DPOexternalusers@epo.org. EPO employees should contact the delegated data controller at dpl.pd44@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 the right to seek legal redress under Article 50 DPR.