Data Protection Statement on the processing of personal data within the team and service quality management in the interpreting area (4.4.3.2)

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 contained **in 443 Team and quality management in interpreting area**.

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

The personal data of the interpreters employed at 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 (cf. Art. 1,2 and 3 of the "Conditions of employment for interpreters at the European Patent Office", Codex, Part 2f).

The interpreting department doesn't advertise any vacancies and regularly receives spontaneous applications from freelance interpreters who would like to join the EPO interpreter pool. Candidates usually send an application letter or a CV by email to the EPO (Dept. 4.4.3.2 "Interpreting and Central Support"), i.e. to the generic Outlook Mailbox (Interpreting) or directly to HoD 4.4.3.2 or to the 4.4.3.2 staff member who is concerned with this process.

Applications from candidates who are not found to be suitably qualified are deleted immediately after they were informed about this. Candidates who are found to be suitably qualified are then asked to send their CVs (if missing) and degree certificates.

The collected personal data are then stored in a dedicated and access-restricted folder on the W-Drive and are processed in IAS (Interpreter Administration System) for registering the new users and to provide them the access to a dedicated MS Teams page.

For ensuring the required quality of the delivered interpreting services, evaluation reports are drawn up on a regular basis. These data are stored in a dedicated and access-restricted folder on SharePoint.

*Art. 10 of the "Conditions of employment for interpreters at the European Patent Office", Codex, Part 2f.

The processing of personal data is necessary for:
- keeping a pool of accredited and appropriately qualified interpreters;
- quality management purposes (induction of newly selected candidates 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 the application documents and any CVs, degree certificates
- title, first and last name, address, professional domicile, address for tax purposes, phone number, mobile phone number, fax, e-mail address, place and date of birth, nationality, bank details, working languages, education data, specialization/preferences, professional experience, references senior EPO interpreters), mother tongue, Bahncard (yes/no), tax number, availabilities (when interpreters were (not) available, when they worked for the EPO) – these data are contained in IAS
- detailed evaluation reports.

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the DG4 - PD 44 – General Administration acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in the management of the respective initiative, project, activity of 443

External contractors involved in 443 interpreting services, including access the personal data.

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

The personal data of freelance interpreters are accessible to:

- HoD 4.4.3.2
- the 4.4.3.2 staff member responsible for the process
- (in case of applications coming in via the generic Outlook Mailbox Interpreting) all 4.4.3.2 staff members responsible for interpreter administration.

EPO external technicians involved in the organisation of the oral proceedings, they get weekly overviews for the purpose of enabling the oral proceedings.

Certain types of personal data (name, address, monthly remuneration plus the relevant internal tax (i. e. gross and net of tax) are sent to national tax/financial authorities in the interpreters' countries of residence (see Art. 14 (2) of the Conditions of Employment for Interpreters at the EPO, Codex, Part 2f)).

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.

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 following base security measures generally apply:
All personal data related to IAS are stored in secure IT applications according to the security standards of EPO. These include:

- User authentication: internal access (by D443) is based on Windows authentication, with Single Sign On, based on active directory groups. External access by interpreters is made via IAS External. Access is done via either the JUNIPER portal (https://telework.epo.org/languageservice), where interpreters enter their Windows user name and password to login. Since 2021, IAS External has also been defined as an Azure application. 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 public page of IAS External to submit a request for interpreters.
- 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

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).

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.

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 on the basis of Article 5(a) and (b) DPR.
(aa) Processing is necessary for the Office's 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:
Article 14 EPC: "Languages of the European Patent Office, European patent applications and other documents".
Article 31 EPC: "Languages of the Administrative Council".
Article 1 of the Conditions of employment for interpreters at the European Patent Office, Codex, Part 2f

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 (quality checks).
Application documents, CVs and degree certificates are directly deleted after examination of the application or, in the case of sufficiently qualified candidates, are kept for max. 5 years. For non-EPO languages, these personal data are kept for 10 years.

Personal data of interpreters who are working for the EPO or have started doing so are kept for the duration of the employment relation with the EPO

Interpreter contracts and declarations regarding social security status (on paper until 2019) have to be kept for additional 10 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_pd44epo.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 the right to seek legal redress under Article 50 DPR.