Data protection statement on the processing of personal data within the framework of the user satisfaction surveys.

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 user satisfaction surveys are targeted at applicants and external representatives who have had dealings with the EPO, and they are carried out by external processors. The sample of potential respondents prepared by the EPO normally includes data only from publicly available sources. Should this data not be sufficient for the external processor to contact the potential respondent, the external processor looks for further contact details in other publicly available sources.

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

This data protection statement relates to the processing of personal data during the user satisfaction surveys.

Statistically solid and representative figures about user satisfaction with products and services of the EPO is an ISO 9001 requirement of EPO's certified Quality Management System and can only be achieved through quantitative surveys with a large number of interviews among both applicants and external representatives. The objective of this processing activity is to measure the level of users' satisfaction, such as by type of user, in order to identify the follow-up measures and actions to be taken to improve the quality of the core products and services provided by EPO. Contact details of the target users, including name, company, telephone/fax number and e-mail address, if available, need to be extracted from EPO databases and processed in order to make the interviews possible.

All contact details extracted from EPO databases for the user satisfaction surveys are publicly available, e.g. through the EPO register, with one exception:

- For the user satisfaction survey on search services, a part of the sampled applications may not have been published yet at the date of the interview carried out by the external processor. The contact details, including personal data, of said applications are therefore not yet publicly available. However, the EPO considers it relevant to have user feedback from recent searches. Disregarding unpublished applications would negatively affect the goal of the surveys, which is to gather user feedback on the current performance of the EPO.

Personal data may be part of the contact details included in the different samples of potential respondents that are transferred to the external processor conducting the interviews.

The EPO uses an initial external processor to transfer the samples to a second external processor. According to the first external processor, all transfers uploaded from the EU (as determined from the client IP address) will be stored on servers in the EU. The EPO encrypts and password-protects all files sent.

The second external processor has been appointed to conduct these surveys and produce statistical reports under the instructions of the EPO. Potential respondents (i.e. users having received/used EPO products and services before the survey) are contacted via e-mail and/or telephone and reply to the questions on a voluntary basis.

The second external processor uses the contact details received from the EPO to reach the potential respondents. These contact details, however, are not always sufficient. The second external processor complements the contact details with further information, sometimes including personal data, from their own databases (from former and current surveys), from the Internet (e.g. LinkedIn, webpages of the companies) or gathered during contacts with respondents through various communication channels such as phone calls, emails, etc. The responses are collected in order to perform statistical processing to explore cause-effect relationships related to satisfaction with the products and services covered by each particular survey. As a result of the processing, statistical reports are produced. These reports contain the answers in an anonymous and aggregated form, in a manner that does not allow individual responses to be identified. The reports are then made available to EPO top management and further staff involved in the analysis of the results.

Neither the EPO nor the external processors use the personal data for any other purpose than carrying out the survey and collecting, aggregating and further analysing the results thereof.

2. What personal data do we process?

For both applicants and external representatives, the following (personal) data, if available, are processed by the EPO, the first and second external processors:

- full name of the potential respondent
- company name
- (postal) address
- telephone number
- email address
- fax number
- contributions provided by users in the survey

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of DG 1's PD 1.5 Customer Journey and Key Account Management, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the User Satisfaction Survey (USS) programme.

External processors involved in providing a transfer platform and conducting the interviews process personal data, which can include accessing it.

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

The preparation of the different samples of potential respondents involves different departments at the EPO.

The samples are then transferred to the second external processor using the first external processor.

The second external processor processes the personal data within its offices in the EU.

Personal data are disclosed on a need-to-know basis to the EPO staff working in Directorates involved in preparing the different samples of potential respondents, which can include manual checks of samples. Such data may also be disclosed on a need-to-know basis to other EPO staff, e.g. to Directorate 521 (Patent Law & Procedures) in case of a complaint that requires their input.

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 stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients.

User personal data are stored on systems located on EPO premises. EPO staff store and process user personal data according to the EPO Data Protection Rules (CA/D 5/21) and the EPO Information Security Guidelines (Circular 382 - Codex 1b).

Regarding the transfer to the second external processor using the first external processor, during an upload, data are stored on the first external processor's servers, and during a download, transfers are encrypted, password-protected and then sent over a secured connection (https).

The second external processor is bound by confidentiality according to the terms of the contract. They 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.

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

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 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 5 [a] 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 Office's management and functioning).

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.

At the EPO, personal data will be kept until completion of a second cycle of user satisfaction surveys and the publication of its results, i.e. a maximum of 5 years. Personal data will then be deleted.

Regarding the first external processor, the uploaded file or files (the upload) through their website are stored on their servers for a period of 7 days by default, afterwards the upload is automatically deleted.

The second external processor keeps personal data for the whole duration of their contract with the EPO for further user surveys. According to this contract, the external processor shall, upon termination of the contract, either completely and irrevocably delete any EPO data or return back to the EPO all EPO data and storage media including any copies thereof, unless the external processor is obligated by applicable law to further store EPO data, in which case the contractor shall inform the EPO accordingly in writing.

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 at DPOexternalusers@epo.org.

You can also contact our Data Protection Officer at dpo@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.