Data protection statement on the processing of personal data in the context of the Deep Tech Finder Application

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.

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

This data protection statement relates to the processing of personal data within the EPO Deep Tech Finder Application (DTF APP). This data protection statement explains the way in which the EPO may have access to personal data of users of the Web application or the mobile application on Apple iOS or Google Android.

The Deep Tech Finder dataset is designed to allow the public to find investment-ready startups that have filed patent applications at the EPO. The startups database is provided by an external provider located in the European Union, and complemented by matched EPO data on published European patent applications. A Data Protection Agreement (DPA) has been signed with this external provider in which it commits to complying with the EPO Data Protection Rules.

The processing is not intended to be used for any automated decision making, including profiling. 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.

2. What personal data do we process?

Personal data which are processed on the EPO servers when users access the DTF APP are:

- the IP address of the user
- browser user agent
- application traffic for delivering Deep Tech Finder data to the screen

These data are automatically erased 90 days after connection.

The user has access to general information on the DTF APP and the following personal data are processed:

- names and surnames of investors when those investors are individuals
- geographical distribution of the startups (mapping)

When the startup is no longer categorised as such, this data is erased and no longer accessible.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Chief Economist acting as the EPO's delegated data controller.

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

The personal connection data are disclosed on a need-to-know basis to EPO staff and external IT contractors for maintenance and support purposes.

Personal connection 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.

The information and personal data made available through the DTF APP is available to the public.

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 to the above-mentioned recipients only.

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 data centre, 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.

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 restricted access.

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.

For the use of EPO Mobile Apps, personal data processed by Apple and the Apple AppStore or by Google and the Google Play store do not form part of this data protection statement. You will have entered into separate data protection and privacy agreements with those organisations, which act separately as Data Controllers.

Google Privacy Policy: https://policies.google.com/privacy
Apple Privacy Policy: https://www.apple.com/legal/privacy

For the avoidance of doubt, the EPO receives no personal information about the users of these App Stores.

The EPO receives:

- the number of app downloads
- the general geographic region of the downloads

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 CEU-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.

For the end users of the DTF APP, it is essential to report which IP address is affected in order to process this request.

Please bear in mind that data protection is not an absolute right. It must always be balanced against other fundamental rights and freedoms and there may be circumstances where one or more of a data subject's rights may be refused. You can find further information on this topic here.

These rights may also be restricted for a temporary period of time on the legitimate grounds laid down in Article 25 DPR (e.g. according to Article 25(1) DPR, "… to safeguard … (g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority" or "(h) the protection of the data subject or the rights and freedoms of others") by legal acts adopted at the level of at least the President of the Office or the President of the Boards of Appeal, or under Circular No. 420 on Implementing Article 25 of the Data Protection Rules. The Circular provides that any such restriction must be limited in time and proportionate and must respect the essence of the data subject's rights.

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 5a 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 EPO'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.

End user data is retained for 90 days after it is first collected. The erasure is done automatically. App content data is kept for as long as the startup is categorised as such.
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.

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.