**Data protection statement on the processing of personal data for ANSERA-BASED SEARCH tool for National Patent Offices**

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 record of processing activity relates to the management of the Ansera-based Search tool used for the registered users, who are patent examiners from National Patent Offices. The data in scope of the Ansera-based Search tool is limited to published patent information only. Ansera-based Search offers registered users the possibility of searching prior-art patent information data by using complex search expressions. Search-related information and annotations entered by a user are visible only to the user him/herself and are not shared to any other user, with the exception of administrator users who can access other users' annotations. NPO users enabled to use Ansera-based Search will be priorly provisioned into EPO's identity management system via the Single Access Portal. More information concerning Ansera-based Search can be found in the technical documents published on the Single Access Portal (epn.epo.org).

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

This data protection statement relates to the processing of personal data within the context of the Ansera-based Search tool for National Patent Offices.

Personal data are processed for the following purposes:

- delivering to National Offices patent examiners a Search tool.
- operating and maintaining the Ansera-based Search tool itself.
- monitoring the Ansera-based Search tool's availability and performance.
- performing technical troubleshooting and managing security incidents.
- capacity planning and licence management purposes.

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?**

Categories of personal data for Ansera-based Search registered users comprise:

- User Account Information: user id, application specific user role, membership permissions.

- Browsing Information: IP address, URL, cookie information, browser user agent, browser type, browsing date and time.
- Network/Application interaction data: session content, session details, session metadata, including dossier session details.
- System Logs: audit logs, file data, firewall/router/switch logs, ports, registry data, running.
- Processes, System-, Application-, Security-related Server Logs, Transaction- related details, Web Servers Logs.
- Personal Identification: full name, professional e-mail address, country.
- Search query and annotations.
- Physical and/or digital identifiable assets used.

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

Personal data are processed under the responsibility of EPO Principal Directorate 4.5 Chief Technology Officer, acting as the EPO's delegated data controller.

External contractors involved in providing services may also process personal data, which can include accessing it.

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

Personal data are disclosed on a need-to-know basis to the EPO staff working in BIT (Kubernetes Test & Deployment Automation team, Operations, 4.5.2 IT Cooperation project team, National Offices Support team, Ansera team and software developers, Ansera-based Search team and software developers).

Personal data may be disclosed to third-party service providers when providing the service as well as for maintenance, support, and development purposes, as well as for analysing user requirements for planning purposes.

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.

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.

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 a 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. 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).

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 the 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) of the DPR i.e. 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.

The IT infrastructure provides plenty of logged information related to the cloud resources located within the Ansera-based Search project. There are two default storage buckets created automatically in GCP, namely "_Default" and "_Required"; their retention periods are defined as 30 days for "_Default" and 400 days for "_Required".

The IT infrastructure has a feature to check the user's queries for eventual malicious content before such queries reach the Search application. These logs are natively available to the Search system for 30 days and forwarded to the EPO's Information Security team log repository system.

The selection of GCP logs is forwarded to the EPO's Information Security team Central Log Repository and the retention period for these logs is 12 months.
Search Tool's operational application logs – including received requests – are logged for troubleshooting, performance and security monitoring purposes. Access to operational logs – within the Ansera-based Search cluster – is restricted. Such logs are not forwarded to the EPO's Information Security Central Log Repository. Search's application components which log search markers are configured to replace those entries with common placeholder text. The retention of operational application logs is 12 months.

Search data is linked to the lifecycle of the user accounts. User accounts are managed (created and deleted) by the administrator of the NPO under a user administration feature.

Search data such as markers, bibliographic data, User Session State data, concepts, annotations, aROSS are kept under EPO EKMS encryption for an indefinite period. Annotations made by users on a dossier within the Search Tool are stored until the user deletes the dossier and can be deleted on request.

Search Tool's user credentials are kept in Search's master system (Single Access Portal) until flagged inactive; when flagged inactive, the EPO identity management system will keep such credentials for additional 30 days and ultimately will erase them.

**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 *DPOexternalusers@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.