Data protection statement on the processing of personal data via Web Search Assistant (WSA) for National 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 data protection statement relates to processing of personal data done via the Web Search Assistant (WSA), a tool offered to and used by registered users who are National Patent Offices patent examiners enabled to use the EPO's Search tool for National Patent Offices (a.k.a. ANSERA-based Search).
The WSA is a search tool that improves the examiners' search experience on the internet; it works as a browser plugin pinned as an extension in Google Chrome. It is linked to ANSERA-based SEARCH (AbS):
• You can use the AbS markers to search and highlight.
• You can add a document found online and available in our in-house collection to a drawer in AbS.
It indicates the timeliness and availability of the online results and provides a VIN bar for browsing the highlighted hits.
The WSA enables registered users to identify relevant prior-art patent and non-patent literature information in the webpages they browse, by using complex search expressions. The data which can be searched via WSA is limited to content of webpages browsed by the user with the WSA plugin enabled.
Search related information entered by a user is visible only to the user themselves and is not shared to any other user.

NPO users enabled to use the WSA will be priorly provisioned into the EPO's identity management system via the Single Access Portal. More information on the WSA can be found in the technical documentation 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 via the Web Search Assistant (WSA) for National Patent Offices.
Personal data are processed for the following purposes:

- delivering to National Offices patent examiners a Web Search Assistant tool;
- operating and maintaining the WSA tool itself;

- monitoring the WSA tool's availability and performance;
- performing technical troubleshooting and managing security incidents;
- for capacity planning and licence management reasons.

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 following categories of WSA registered users' personal data are processed:

- Personal Identification: full name, professional e-mail address, country.
- 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, search query, webpage data showing potential prefiltered patent identification numbers or non-patent literature identification fields (e.g. doi, author, publication date, etc).
- Network/Application interaction data: session content, session details, session metadata, including Ansera-based Search 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.

3. Who is responsible for processing the data?

Personal data is processed under the responsibility of the CIO/Principal Director BIT 4.6, acting as the EPO's delegated data controller.
Personal data is processed by the EPO staff involved in managing the WSA project.
External contractors involved in IT operation and maintenance, software development and IT Security 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 a limited number of EPO BIT staff members working in the teams: Search Products, IT Cooperation Partnerships, Information Security and Cloud Operations.

Personal data may be disclosed to third-party service providers when providing the service; for maintenance, support, troubleshooting, bug fixing and development purposes; and to analyse user requirements.

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.

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. 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).

The EPO has appropriate security measures in place to detect and remediate eventual security vulnerabilities affecting the WSA software.

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.

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 DP_BIT@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) 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.

The Web Search Assistant and the Search Tool for National Patent Offices are parts of EPO IT Cooperation Programme adopted by the Administrative Council in June 2024; see CA/55/24.

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 logs information related to the cloud resources located within the AbS project hosting the WSA component. A selection of these GCP logs are forwarded to the EPO Information Security team and the retention period for these logs is 12 months.

The IT infrastructure has a feature to check the user's queries for potential malicious content or automated traffic before such queries reach the WSA application.

Search Tool's operational application logs – including received requests – are logged for troubleshooting, performance and security monitoring purposes. Such logs are not forwarded to the EPO Information Security team . The retention of operational application logs is 12 months.

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

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 DP_BIT@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.