

Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen des ANSERA-basierten Recherchetools SEARCH für nationale Patentämter

Der Schutz Ihrer Privatsphäre ist für das Europäische Patentamt (EPA) von höchster Bedeutung. Wir sind bei der Erfüllung unserer Aufgaben und der Erbringung unserer Dienstleistungen dem Schutz Ihrer personenbezogenen Daten sowie der Wahrung Ihrer Rechte als betroffener Person verpflichtet. Alle Daten persönlicher Art, die Sie direkt oder indirekt identifizieren, werden rechtmäßig, fair und mit der gebotenen Sorgfalt verarbeitet.

Die nachstehend beschriebenen Verarbeitungen erfolgen nach den Datenschutzvorschriften ([DSV](#)) des EPA.

Die Informationen in dieser Erklärung werden Ihnen gemäß den Artikeln 16 und 17 DSV bereitgestellt.

Dieses Verzeichnis von Verarbeitungstätigkeiten bezieht sich auf die Verwaltung des ANSERA-basierten Recherchetools SEARCH, das von registrierten Nutzern, d. h. Patentprüfern aus nationalen Patentämtern, genutzt wird. Das ANSERA-basierte Recherchetool SEARCH enthält nur veröffentlichte Patentinformationen. Es bietet registrierten Nutzern die Möglichkeit, mithilfe komplexer Suchbegriffe in Patentinformationsdaten des Stands der Technik zu recherchieren. Suchbezogene Informationen und vom Nutzer eingegebene Anmerkungen sind nur für den jeweiligen Nutzer sichtbar und werden nicht an andere Nutzer weitergegeben. Eine Ausnahme hiervon bilden lediglich Nutzer mit Administratorrechten, die auch auf die Anmerkungen anderer Nutzer zugreifen können. Nutzer in Non-Profit-Organisationen, die für die ANSERA-basierte Recherche berechtigt sind, werden zuvor über das einheitliche Zugangsportale in das Identitätsmanagementsystem des EPA eintragen. Weitere Informationen zum ANSERA-basierten Recherchetool SEARCH sind den technischen Unterlagen zu entnehmen, die im einheitlichen Zugangsportale (epn.epo.org) veröffentlicht werden.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Diese Datenschutzerklärung bezieht sich auf die Verarbeitung personenbezogener Daten im Rahmen des ANSERA-basierten Recherchetools SEARCH für nationale Patentämter.

Personenbezogene Daten werden zu folgenden Zwecken verarbeitet:

- Bereitstellung eines Recherchetools für die Patentprüfer der nationalen Ämter
- Betrieb und Pflege des ANSERA-basierten Recherchetools SEARCH
- Überwachung von Verfügbarkeit und Leistung des ANSERA-basierten Recherchetools SEARCH
- Durchführung technischer Fehlerbehebungen und Verwaltung von Sicherheitsvorfällen
- Kapazitätsplanung und Lizenzverwaltung

Die Verarbeitung ist nicht zur Verwendung für eine automatisierte Entscheidungsfindung (einschließlich Profiling) gedacht.

Ihre personenbezogenen Daten werden an Empfänger außerhalb des EPA, die nicht unter Artikel 8 (1), (2) und (5) DSV fallen, nur dann übermittelt, wenn ein angemessenes Schutzniveau gewährleistet ist. Ist dies nicht der Fall, kann eine Übermittlung nur erfolgen, sofern geeignete Garantien vorgesehen sind und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen oder Ausnahmen für bestimmte Fälle nach Artikel 10 DSV zur Anwendung kommen.

2. Welche personenbezogenen Daten verarbeiten wir?

Die folgenden Kategorien von personenbezogenen Daten registrierter Nutzer des ANSERA-basierten Recherchertools SEARCH werden verarbeitet:

- Nutzerkontodaten: Nutzer-ID, anwendungsspezifische Nutzerrolle, Mitgliedschaftsberechtigungen
- Browsing-Informationen: IP-Adresse, URL, Cookie-Informationen, Browser-Nutzer-Agent, Browser-Typ, Browsing-Datum und -Uhrzeit
- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsinhalt, Sitzungsdetails, Sitzungsmetadaten einschließlich aktenbezogenen Sitzungsdetails
- Systemprotokolle: Überwachungsprotokolle, Dateidaten, Firewall-/Router-/Switch-Protokolle, Port-Nummern, Registry-Daten, laufende Prozesse
- system-, anwendungs- und sicherheitsbezogene Server-Protokolle, transaktionsbezogene Details, Webserver-Protokolle
- persönliche Identifikation: vollständiger Name, E-Mail-Adresse (geschäftlich), Land
- Suchabfrage, Anmerkungen
- physische und/oder digitale identifizierbare Anlagen

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung der Hauptdirektion Chief Technology Officer (HD 4.5) verarbeitet, die als delegierter Datenverantwortlicher des EPA handelt.

Externe Auftragnehmer, die an der Bereitstellung der Dienste beteiligt sind, können die personenbezogenen Daten ebenfalls verarbeiten und gegebenenfalls auf sie zugreifen.

4. Wer hat Zugriff auf Ihre personenbezogenen Daten und für wen werden sie offengelegt?

Personenbezogene Daten werden bedarfsorientiert für EPA-Bedienstete in BIT offengelegt (Team Kubernetes-Test- & -Bereitstellungsautomatisierung, Team IT-Zusammenarbeit (4.5.2) Team Unterstützung nationaler Ämter, Team Ansera sowie Softwareentwickler, Team Ansera-basierte Recherche sowie Softwareentwickler).

Personenbezogene Daten können für Drittanbieter offengelegt werden, die den Dienst anbieten, für Wartungs-, Unterstützungs-, und Entwicklungszwecke sowie zur Analyse der Nutzeranforderungen für Planungszwecke.

Personenbezogene Daten werden nur an entsprechend befugte Personen weitergegeben, die für die erforderlichen Verarbeitungsvorgänge zuständig sind. Sie werden nicht für andere Zwecke verwendet oder anderen Empfängern gegenüber offengelegt.

5. Wie schützen wir Ihre personenbezogenen Daten?

Wir ergreifen geeignete technische und organisatorische Maßnahmen, um Ihre personenbezogenen Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung bzw. unbefugtem Zugang zu schützen. Alle personenbezogenen Daten werden in sicheren IT-Anwendungen gemäß den Sicherheitsstandards des EPA gespeichert. Angemessene Zugriffsberechtigungen werden individuell nur den oben genannten Empfängern gewährt.

Für Systeme, die in den Räumlichkeiten des EPA gehostet werden, gelten allgemein die folgenden grundlegenden Sicherheitsmaßnahmen:

- Benutzerauthentifizierung und Zugriffskontrolle (z. B. rollenbasierte Zugriffskontrolle auf die Systeme und das Netzwerk,
- Bedarfsorientiertheit und Least-Privilege-Prinzip)
- logische Sicherheitshärtung der Systeme und Geräte sowie des Netzwerks
- physischer Schutz: EPA-Zugangskontrollen, zusätzliche Zugangskontrollen für das Rechenzentrum, Regeln für das
- Abschließen von Büros
- Übertragungs- und Eingabekontrollen (z. B. Auditprotokollierung, System- und Netzwerküberwachung)
- Reaktion auf sicherheitsrelevante Vorfälle: Rund-um-die-Uhr-Überwachung auf Vorfälle, Sicherheits-experte in Bereitschaft

Das EPA verwendet grundsätzlich ein papierloses Verwaltungssystem. Wenn dennoch Papierakten mit personenbezogenen Daten in den EPA-Gebäuden gelagert werden müssen, werden sie an einem sicheren verschlossenen und zugangsbeschränkten Ort aufbewahrt.

Für personenbezogene Daten, die mit nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, haben sich die die personenbezogenen Daten verarbeitenden Anbieter in einer rechtsverbindlichen Vereinbarung verpflichtet, die sich aus dem anwendbaren Datenschutzrahmen ergebenden Verpflichtungen zu erfüllen. Das EPA hat außerdem eine Überprüfung der Datenschutz- und Sicherheitsrisiken durchgeführt. In diesen Systemen müssen geeignete technische und organisatorische Maßnahmen umgesetzt worden sein, wie z. B. physische Sicherheitsmaßnahmen, Zugriffs- und Speicherkontrollmaßnahmen, Sicherung von ruhenden Daten (z. B. durch Verschlüsselung), Benutzer-, Übertragungs- und Eingabekontrollmaßnahmen (z. B. Netzwerk-Firewalls, Network Intrusion Detection System (IDS), Network Intrusion Protection System (IPS), Audit-Protokollierung) und Transportkontrollmaßnahmen (z. B. Sicherung von Daten bei der Übertragung durch Verschlüsselung).

6. Wie können Sie Auskunft über Ihre Daten erlangen, Ihre Daten berichtigen oder Ihre Daten erhalten? Wie können Sie die Löschung Ihrer Daten verlangen oder ihre Verarbeitung beschränken bzw. ihr widersprechen? Können Ihre Rechte beschränkt werden?

Sie haben das Recht, Auskunft über Ihre personenbezogenen Daten zu erlangen, Ihre Daten zu berichtigen und Ihre Daten zu erhalten, das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, sowie das Recht, Ihre Daten löschen zu lassen und die Verarbeitung Ihrer Daten zu beschränken und/oder ihr zu widersprechen (Artikel 18 bis 24 DSV).

Wenn Sie von einem dieser Rechte Gebrauch machen möchten, wenden Sie sich bitte schriftlich unter DPOexternalusers@epo.org an den delegierten Datenverantwortlichen. Damit wir schneller und genauer reagieren können, sollten Sie uns mit Ihrem Antrag stets bestimmte Vorabinformationen übermitteln. Wir empfehlen Ihnen daher, dieses [Formular](#) auszufüllen und es mit Ihrem Antrag einzureichen.

Wir werden Ihren Antrag baldmöglichst und in jedem Fall innerhalb eines Monats nach Eingang des Antrags bearbeiten. Gemäß Artikel 15 (2) DSV kann dieser Zeitraum jedoch um zwei Monate verlängert werden, wenn es aufgrund der Komplexität und der Zahl der eingegangenen Anträge erforderlich ist. Wir werden Sie in diesem Fall entsprechend informieren.

7. Auf welcher Rechtsgrundlage basiert die Verarbeitung Ihrer Daten?

Personenbezogene Daten werden gemäß Artikel 5 a) DSV verarbeitet: Die Verarbeitung ist für die Wahrnehmung einer Aufgabe in Ausübung der amtlichen Tätigkeit der Europäischen Patentorganisation oder in rechtmäßiger Ausübung dem Verantwortlichen übertragener öffentlicher Gewalt, was die für die Verwaltung und die Arbeitsweise des Amts notwendige Verarbeitung einschließt, erforderlich.

8. Wie lange speichern wir Ihre Daten?

Personenbezogene Daten werden nur so lange gespeichert, wie es für die Zwecke der Verarbeitung erforderlich ist.

Die IT-Infrastruktur stellt eine Vielzahl an Protokolldaten bereit, die in Verbindung mit den Cloud-Ressourcen für das ANSERA-basierte Rechercheprojekt anfallen. In GCP werden automatisch zwei Standard-Speicher-Buckets erzeugt: "_Default" und "_Required"; dabei beträgt die Aufbewahrungsdauer für Daten in "_Default" 30 Tage, für "_Required" 400 Tage.

Die IT-Infrastruktur ist mit einer Funktion ausgestattet, die Benutzerabfragen vor Erreichen der SEARCH-Anwendung auf etwaige schädliche Inhalte überprüft. Die zugehörigen Protokolle sind für 30 Tage im SEARCH-System nativ verfügbar und werden an das Protokoll-Repository-System des Informationssicherheitsteams weitergeleitet.

Die Auswahl der GCP-Protokolle wird an das zentrale Protokoll-Repository des Informationssicherheitsteams weitergeleitet und für einen Zeitraum von 12 Monaten aufbewahrt.

Die Betriebsprotokolle für das Recherchetool SEARCH – einschließlich der empfangenen Anfragen – werden zum Zwecke der Fehlerbehebung, Leistungs- und Sicherheitsüberwachung aufgezeichnet. Der Zugriff auf Betriebsprotokolle innerhalb des ANSERA-basierten Recherchetool-Clusters ist beschränkt. Die betreffenden Protokolle werden nicht an das zentrale Protokoll-Repository der EPA-Informationssicherheit weitergeleitet. SEARCH-Anwendungskomponenten zur Protokollierung von bei der Recherche gesetzten Markierungen werden so konfiguriert, dass die betreffenden Einträge durch allgemeinen Platzhaltertext ersetzt werden. Die Aufbewahrungsdauer für die Betriebsprotokolle der Anwendung beträgt 12 Monate.

Suchdaten werden mit dem Lebenszyklus der Nutzerkonten verknüpft. Nutzerkonten werden vom Administrator der Non-Profit-Organisation über eine Nutzerverwaltungsfunktion verwaltet (angelegt und gelöscht).

Suchdaten wie Markierungen, bibliografische Daten, Statusdaten zur Nutzersitzung, Konzepte, Anmerkungen und aROSS werden mittels EPA-EKMS-Verschlüsselung für einen unbegrenzten Zeitraum aufbewahrt. Anmerkungen, die von Nutzern des Recherchetools SEARCH in einer Akte vorgenommen werden, bleiben so lange gespeichert, bis der Nutzer die Akte löscht. Alternativ können sie auch auf Antrag gelöscht werden.

Nutzerberechtigungen für das Recherchetool werden im SEARCH-Mastersystem (einheitliches Zugangsportale) gespeichert, bis sie als inaktiv markiert werden. Entsprechend markierte Berechtigungsdaten werden im Identitätsmanagementsystem des EPA für weitere 30 Tage aufbewahrt und anschließend gelöscht.

9. Kontaktinformationen

Bei Fragen zur Verarbeitung Ihrer personenbezogenen Daten wenden Sie sich bitte schriftlich an den delegierten Datenverantwortlichen unter DPOexternalusers@epo.org.

Sie können sich auch an unseren Datenschutzbeauftragten unter DPOexternalusers@epo.org wenden.

Überprüfung und Rechtsmittel

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihre Rechte als betroffene Person verletzt, sind Sie berechtigt, gemäß Artikel 49 DSV einen Antrag auf Überprüfung durch den Verantwortlichen zu stellen, und falls Sie mit dem Ergebnis der Überprüfung nicht einverstanden sind, können Sie gemäß Artikel 50 DSV Rechtsmittel einlegen.