Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen von Beschaffungstätigkeiten

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 des EPA (DSV).

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

In dieser Datenschutzerklärung wird erläutert, wie das EPA personenbezogene Daten im Rahmen von Beschaffungstätigkeiten des EPA verarbeitet.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Diese Datenschutzerklärung betrifft die Verarbeitung personenbezogener Daten im Rahmen von Beschaffungstätigkeiten.

Unternehmen, die ein Angebot für Ausschreibungen des EPA abgeben möchten, müssen auf der eTendering-Plattform des EPA ein Nutzerprofil registrieren. Dazu müssen eine gültige E-Mail-Adresse und Kontaktdaten angegeben werden.

Nach der Registrierung können Unternehmen die eTendering-Plattform nutzen, um Verdingungsunterlagen herunterzuladen, wirksame Angebote einzugeben und rechtsgültige elektronische Angebote abzugeben. Die Angebote können vom Unternehmen/Bieter bereitgestellte personenbezogene Daten wie Namen, Kontaktdaten und Lebensläufe von Mitarbeitern enthalten.

Die Hauptdirektion Beschaffung und Lieferantenmanagement (HD 4.7) verarbeitet die Daten über die eTendering-Plattform, um mit den bietenden Unternehmen zu kommunizieren und Ausschreibungsverfahren durchzuführen.

Neue Lieferanten, die den Zuschlag für ein Angebot und einen Auftrag erhalten haben, müssen sich registrieren, um sich im Beschaffungs- und Sourcingportal des EPA anzumelden, das zur Verbesserung der Partnerschaft und Transparenz sowie zur Optimierung der Zusammenarbeit zwischen dem EPA und seinen Lieferanten entwickelt wurde. Bei dieser Registrierung muss zusätzlich zu den Unternehmensdaten ein Mitarbeiter des Lieferanten als Ansprechpartner mit den entsprechenden Daten (Name, Kontaktdaten) angegeben werden. Bei Vertragsabschluss wird der Vertrag elektronisch über die DocuSign-Integration unterzeichnet.

Registrierte Lieferanten können das Beschaffungs- und Sourcingportal des EPA nutzen, um ihre Unternehmensdaten sowie ihre Kontaktdaten einzugeben und zu aktualisieren. Darüber hinaus können neue oder geänderte Verträge unterzeichnet oder angezeigt werden.

HD 4.7 verarbeitet die Daten über das Beschaffungs- und Sourcingportal des EPA, um Verträge abzuschließen und Beschaffungstätigkeiten mit Lieferanten durchzuführen.

Personenbezogene Daten (Name, Kontaktdaten) werden bedarfsorientiert an die Rechtsabteilung (Vertragsabschluss) oder die Finanzabteilungen des EPA (Beschaffungstätigkeiten) weitergegeben.

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

Personenbezogene 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?

Folgende Kategorien personenbezogener Daten werden verarbeitet:

Tätigkeiten in Bezug auf eTendering:
Kontaktdaten; geschäftliche E-Mail-Adresse; Funktion/Rolle; digitale Signatur; vollständiger Name; Signatur; System-, Anwendungsinformationen; zusätzliche Informationen, die ggf. während des Austauschs bereitgestellt werden; sicherheitsrelevante Serverprotokolle; Konto-Passwort, Nutzerkennung

Tätigkeiten in Bezug auf Beschaffung und Sourcing des EPA:
Kontaktdaten; geschäftliche E-Mail-Adresse; Funktion/Rolle; Ausweis-/Passbild; Ausweisdaten; digitale Signatur; vollständiger Name; Signatur; System-, Anwendungsinformationen; zusätzliche Informationen, die ggf. während des Austauschs bereitgestellt werden; sicherheitsrelevante Serverprotokolle; Konto-Passwort, Nutzerkennung

Tätigkeiten in Bezug auf die elektronische Vertragsunterzeichnung über die DocuSign-Integration:
Kontaktdaten; geschäftliche E-Mail-Adresse; Ausweis-/Passbild; Ausweisdaten; digitale Signatur; vollständiger Name; Signatur; System-, Anwendungsinformationen; sicherheitsrelevante Serverprotokolle

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung der HD 4.7, Beschaffung und Lieferantenmanagement, verarbeitet, die als delegierte Datenverantwortliche des EPA handelt.

Personenbezogene Daten werden von den Bediensteten des EPA verarbeitet, die an der Verwaltung der in dieser Erklärung genannten Tätigkeiten der HD 4.7 beteiligt sind.

Externe Auftragnehmer, die an der eTendering-Plattform oder dem Beschaffungs- und Sourcingportal des EPA 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 der Rechtsabteilung des EPA und in den Finanzabteilungen des EPA weitergegeben.

Personenbezogene Daten können gegenüber externen Dienstleistern zum Zwecke der Datenpflege und der Unterstützung offengelegt werden.

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, Sicherheitsexperten in Bereitschaft

Das EPA verwendet grundsätzlich ein papierloses Verwaltungssystem; wenn dennoch Papierakten mit personenbezogenen Daten in den Räumlichkeiten des EPA gelagert werden müssen, werden sie an einem sicheren verschlossenen und zugangsbeschränkten Ort aufbewahrt.
Wenn Daten outgesourct (z. B. extern gespeichert, zugänglich gemacht und verarbeitet) werden, wird eine Risikobewertung für Datenschutz und Sicherheit durchgeführt, und folgende allgemeine Erklärung könnte aufgenommen werden:

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), Auditprotokollierung) 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).

Externe betroffene Personen, die von einem dieser Rechte Gebrauch machen möchten, wenden sich bitte schriftlich unter DPOexternalusers@epo.org an den delegierten Datenverantwortlichen. Damit wir schneller und genauer darauf antworten 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 unverzüglich, in jedem Fall aber 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?

Die rechtliche Grundlage für die Verarbeitung personenbezogener Daten im Rahmen von eTendering stellt Artikel 5 a) DSV dar, in dem es heißt:
"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"

Die Verarbeitung personenbezogener Daten bei Tätigkeiten im Zuge von Beschaffung und Sourcing des EPA, einschließlich elektronischer Vertragsunterzeichnung über die DocuSign-Integration, erfolgt gemäß Artikel 5 c) DSV, in dem es heißt:
"die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen"

Personenbezogene Daten werden auf der Grundlage folgender Rechtsvorschriften verarbeitet: Finanzordnung des EPA, insbesondere Vergaberichtlinien und Weisung für Verträge

8. Wie lange speichern wir Ihre Daten?

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

Personenbezogene Daten im Zuge von Beschaffungstätigkeiten werden 12 Jahre gespeichert

Personenbezogene Daten, die zur Überprüfung der Identität im Rahmen der elektronischen Signatur verarbeitet werden, werden maximal 90 Tage gespeichert, bevor sie gelöscht werden.

Im Falle einer förmlichen Beschwerde/Rechtsstreitigkeit werden alle Daten, die bei Einleitung der förmlichen Beschwerde/Rechtsstreitigkeit gespeichert waren, bis zum Abschluss des Verfahrens aufbewahrt.

9. Kontaktinformationen

Wenn Sie Fragen zur Verarbeitung Ihrer personenbezogenen Daten haben, wenden Sie sich bitte unter *DPOexternalusers@epo.org* an unseren Datenschutzbeauftragten.

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.