

Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen von EPA-Smartcards

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.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Diese Datenschutzerklärung beschreibt die Verarbeitung personenbezogener Daten im Rahmen der Registrierung und Nutzung von Smartcards. Smartcards sind Kunststoffkarten im Kreditkartenformat, die mit einem Mikroprozessor und einem kleinen Speicher ausgestattet sind. Im Gegensatz zu Passwörtern können wir mit Smartcards die sicherere 2-Faktor-Authentifizierung gewährleisten, die sich auf eine physische Komponente (die Smartcard) und eine Informationskomponente (den PIN-Code) stützt. Smartcards sind handlich, bieten eine fälschungssichere Speicherung von privaten Schlüsseln und digitalen Zertifikaten und sind sehr gut gegen das unberechtigte Löschen oder Kopieren der Zertifikate und Schlüssel geschützt.

Für die Nutzung der folgenden Online-Dienste des EPA ist eine Smartcard erforderlich: Mailbox/My Files, Verwaltungstool, Online-Einreichung (OLF), Online-Einreichung 2.0, MyEPO. Für die Nutzung der Zentralen Gebührenzahlung kann die Smartcard verwendet werden.

Smartcards sind fünf Jahre gültig und werden an Einzelpersonen ausgestellt, damit sie mitgenommen können, wenn der Arbeitgeber wechselt. Bei der Online-Einreichung (OLF) kann eine Smartcard für mehrere Unternehmen gleichzeitig verwendet werden, nicht jedoch bei der Online-Einreichung 2.0 und beim Verwaltungsportal (einschließlich Mailbox und My Files); hier brauchen Sie für jedes Unternehmen eine eigene Karte.

Für die Registrierung einer Smartcard muss ein Online-Formular mit persönlichen Daten, Unternehmensangaben und Kontaktdaten ausgefüllt werden (siehe Abschnitt 2 unten).

Wenn Sie kein/e Vertreter/in sind, haben Sie zwei Möglichkeiten der Identitätsprüfung:

- a. Vorlage einer Kopie des Personalausweises, Reisepasses oder Führerscheins, wenn im Unternehmen keine/n Vertreter/in zur Unterzeichnung des PDF-Formulars befugt und autorisiert ist: dies ist erforderlich, um nachzuweisen, dass die Person, die die Smartcard erhalten soll, eine echte Person ist, und dass die Smartcard nicht mit anderen Unternehmen geteilt wird.
- b. Gegenzeichnung des Formulars durch eine/n Vertreter/in im Unternehmen: ein/e Vertreter/in unterzeichnet das Formular, und das EPA prüft intern, ob diese Person in der Liste der zugelassenen Vertreter eingetragen ist.

Das EPA sendet wöchentlich über das Tool eines externen Anbieters Daten betreffend die Neuregistrierung und die Ersetzung von Smartcards sowie die Auslieferung von Smartcard-Lesegeräten. Der externe Anbieter KPN stellt die Daten der EPA-Nutzer/innen und die Zertifikate auf Chips bereit, personalisiert die Smartcards (indem auf die Rohlinge das EPA-Logo, der Name, die Smartcard-Nummer und das Ablaufdatum aufgebracht

werden) und sendet sie dann (bei Bedarf mit einem Lesegerät) per Einschreiben an den Nutzer bzw. die Nutzerin. Der Anbieter sendet ferner PIN-Schreiben an die EPA-Nutzer/innen über den normalen Postweg.

Personenbezogene Daten werden somit zur Ermöglichung der Zwei-Faktor-Authentifizierung verarbeitet, durch die die Sicherheit der EPA-Online-Dienste erhöht wird.

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?

Folgende Kategorien personenbezogener Daten werden verarbeitet:

EPA-Bedienstete:

- Geschäftliche E-Mail-Adresse
- Vollständiger Name
- Digitales Zertifikat
- Smartcard-Nummer
- Unternehmenseinheit

Externe Personen:

- Reisepassnummer
- Ausweis-/Passfoto
- Angaben im Personalausweis
- Kontopasswort
- Kontaktdaten
- Geschäftliche E-Mail-Adresse
- Mobiltelefonnummer
- Telefonnummern
- Land
- Digitales Zertifikat
- Smartcard-Nummer
- Browser User Agent
- URL
- Browsing-Datum und Uhrzeit
- IP-Adresse
- Nachname
- Geschlecht
- Vorname
- Vollständiger Name
- Unternehmenseinheit
- Bevorzugte Sprache (für die Kommunikation)
- Vertreter-Registrierungsnummer (ID)
- Laufendes Konto

Auftragnehmer:

- Digitales Zertifikat
- Smartcard-Nummer
- Unternehmenseinheit
- Vollständiger Name
- Geschäftliche E-Mail-Adresse

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung des Vizepräsidenten GD 1 Patenterteilungsprozess verarbeitet, der als delegierter Datenverantwortlicher des EPA handelt.

Personenbezogene Daten werden von den Bediensteten des EPA verarbeitet, die an den in dieser Erklärung benannten Prozessen beteiligt sind.

Externe Auftragnehmer, die an der Herstellung, Personalisierung und Auslieferung der Smartcards beteiligt sind, können personenbezogene 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 der Abteilungen D 1.5.1.2 Kundenanfragen und D 1.5.1.1 Key Account Management und Kundenbetreuung offengelegt, und zwar insbesondere an Bedienstete, die in diesen Abteilungen für das Customer-Service-Management (CSM) zuständig sind (siehe Datenschutzerklärung für das Customer-Service-Management (CSM)).

Personenbezogene Daten können für Dritte zum Zweck der Herstellung, Personalisierung und Auslieferung der Smartcards 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. Extern gelten die in der Datenverarbeitungsvereinbarung mit dem externen Anbieter definierten Sicherheitsmaßnahmen.

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, Sicherheitsexperte in Bereitschaft

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); 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 als externer Nutzer bitte schriftlich an DPOexternalusers@epo.org bzw. als interner Nutzer an dg1_dpl@epo.org (delegierte/r Datenverantwortliche/r). Damit wir schneller und genauer darauf antworten können, sollten Sie uns mit Ihrem Antrag stets bestimmte Vorabinformationen übermitteln. Deshalb bitten wir Sie, als *externer* Nutzer dieses [Formular](#) und als *interner* Nutzer dieses [Formular](#) auszufüllen und zusammen 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 EPA notwendige Verarbeitung einschließt, erforderlich.

8. Wie lange speichern wir Ihre Daten?

Das EPA speichert personenbezogene Daten nur so lange gespeichert, wie es für die Zwecke der Verarbeitung erforderlich ist.

Der externe Anbieter speichert die personenbezogenen Daten wie folgt:

- Informationen im Rahmen der Registrierung einer Smartcard (Name, E-Mail-Adresse, Lieferanschrift, Informationen zur Sendungsverfolgung): bis Vertragsablauf
- Transaktionsprotokolle für Zertifikate: sieben Jahre nach Vertragsablauf
- Zertifikatsperrliste (enthält nur die Seriennummern der gesperrten Zertifikate): bis Vertragsablauf
- Informationen zu Zugriffsberechtigungen für EPA-Bedienstete und -Auftragnehmer, die Zugriff auf die Umgebung der Firma KPN haben: bis Vertragsablauf

EPA-Smartcards sind fünf Jahre gültig. Ein abgelaufenes Zertifikat kann als vollständig funktionsuntüchtig betrachtet werden. Es wird eine Zertifikatsperrliste geführt, sodass keine Verarbeitung mit einem für ungültig erklärten Zertifikat möglich ist (z. B. Authentifizierung, Signatur, Verschlüsselung). Das heißt, eine abgelaufene oder für ungültig erklärte Smartcard kann als vom externen Auftragsverarbeiter vollständig deaktiviert betrachtet werden. Ein Zertifikat enthält den Namen der betroffenen Person und kann während diverser Verfahren im Rahmen der Patenterteilung verschiedenen digital signierten Dokumenten hinzugefügt werden. In diesem Zusammenhang ist zu verweisen auf den [Beschluss des Präsidenten des Europäischen Patentamts vom 13. Dezember 2021 betreffend die Verarbeitung personenbezogener Daten im Rahmen des Patenterteilungsverfahrens und damit zusammenhängender Verfahren](#) sowie auf die weiteren [Datenschutzerklärungen zum Patenterteilungsverfahren](#).

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

Bei Fragen zur Verarbeitung ihrer personenbezogenen Daten können sich externe betroffene Personen schriftlich an DPOexternalusers@epo.org (delegierte/r Datenverantwortliche/r) wenden.

EPA-Bedienstete wenden sich an dg1_dpl@epo.org (delegierte/r Datenverantwortliche/r). EPA-Bedienstete können auch unter dpo@epo.org die Datenschutzbeauftragte kontaktieren.

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.