

Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Kundenidentitäts- und Zugriffsmanagement-System (CIAM) von Okta

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.

Diese Datenschutzerklärung betrifft die Verarbeitung personenbezogener Daten in Okta. Das EPA nutzt die cloudbasierte SaaS-Plattform (Software as a Service) von Okta für das Identitäts- und Zugriffsmanagement.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Die Verarbeitung erfolgt bei der Nutzerauthentifizierung über Okta. Die Authentifizierung ist erforderlich, sobald Sie versuchen, sich für einen sicheren Bereich der EPA-Online-Dienste anzumelden, auf den nur mit einer Smartcard oder den Zugangsdaten eines für die Nutzung dieser Dienste eingerichteten Kontos zugegriffen werden kann.

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

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.

2. Welche personenbezogenen Daten verarbeiten wir?

Folgende Kategorien personenbezogener Daten werden verarbeitet:

- Vor- und Nachname
- Smartcard-Nummer
- Sprache
- E-Mail-Adresse
- Benutzername
- Passwort
- Telefonnummer
- Verbindungs-/Standortdaten

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Die Verarbeitung personenbezogener Daten erfolgt unter der Verantwortung unseres Chief Information Officer, der unserer Abteilung Business Information Technology (BIT) angehört und als bevollmächtigter Datenverantwortlicher des EPA handelt.

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

Personenbezogene Daten werden bedarfsorientiert für EPA-Bedienstete (Systemadministratoren) des Referats Informationssicherheit (R. 4.6.2.3) und für einige EPA-Bedienstete der GD 1 zum Zwecke der Kundenunterstützung offengelegt. Sie können ferner bedarfsorientiert zu Wartungs- und Unterstützungszwecken an Okta-Beschäftigte weitergegeben 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, die IT-Sicherheit betreffende 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, Sicherheitsexperte in Bereitschaft

Für personenbezogene Daten, die mit nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, hat Okta sich 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.

Okta übermittelt die personenbezogenen Daten nicht in Länder, die kein angemessenes Datenschutzniveau garantieren.

Okta verfügt über administrative, physische und technische Sicherheitsvorkehrungen, um die Sicherheit, Vertraulichkeit und Integrität von sowohl Kundendaten als auch personenbezogenen Daten zu schützen. Diese Sicherheitsvorkehrungen sind in Oktas Dokumentation zu Vertrauenswürdigkeit und Compliance beschrieben.

Okta ist nach dem [Datenschutz-Rahmen der Asiatisch-Pazifischen Wirtschaftsgemeinschaft für Auftragsverarbeiter](#) zertifiziert und verarbeitet personenbezogene Daten entsprechend.

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).

Gemäß den DSV können Beschränkungen der Rechte betroffener Personen auf der Grundlage des Artikels 25 (1) c), g) und h) DSV

sowie des Rundschreibens Nr. 420 zur Umsetzung von Artikel 25 DSV im Rahmen von Untersuchungen und Prüfungen zur Anwendung kommen, die der Datenschutzbeauftragte im Einklang mit Artikel 43 (1) d) und (2) DSV durchführt.

Wenn Sie von einem dieser Rechte Gebrauch machen möchten, wenden Sie sich bitte schriftlich an den [delegierten Datenverantwortlichen](#), BIT, unter DPOexternalusers@epo.org. Damit wir schneller und genauer 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. Artikel 15 (2) DSV sieht allerdings vor, dass dieser Zeitraum bei Bedarf unter Berücksichtigung der Komplexität und Zahl der eingegangenen Anträge um zwei weitere Monate verlängert werden kann. 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, d. h. wenn die Verarbeitung "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 Amtes notwendige Verarbeitung einschließt, erforderlich" ist.

8. Wie lange speichern wir Ihre Daten?

Vom delegierten Datenverantwortlichen oder dieser Funktion unterstellten Dienstleistungsanbietern erhobene personenbezogene Daten werden nur so lange gespeichert, wie es für die Erreichung der Zwecke erforderlich ist, für die sie erhoben wurden.

Personenbezogene Daten werden für die Dauer des Vertrags mit Okta gespeichert.

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 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.

10. Überprüfung und Rechtsmittel

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihre Rechte als betroffene Person verletzt, haben Sie das Recht, gemäß Artikel 49 DSV einen Antrag auf Überprüfung durch den delegierten Datenverantwortlichen zu stellen, und wenn Sie mit dem Ergebnis der Überprüfung nicht einverstanden sind, haben Sie das Recht, gemäß Artikel 50 DSV Rechtsmittel einzulegen.