

Datenschutzerklärung über die Verarbeitung personenbezogener Daten zur Verwaltung der Zugangskontrolle und der Zugangsausweise im EPA

Der Schutz Ihrer Privatsphäre ist für das Europäische Patentamt (EPA) von höchster Bedeutung. Wir sind dem Schutz Ihrer personenbezogenen Daten und 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 Verarbeitung erfolgt nach den Datenschutzvorschriften des EPA ([DSV](#)).

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

Diese Datenschutzerklärung beschreibt die Verarbeitung personenbezogener Daten im Rahmen der Verwaltung der Zugangskontrolle und der Zugangsausweise im EPA. In dieser Datenschutzerklärung wird erläutert, wie die Verarbeitung erfolgt.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Personenbezogene Daten werden verarbeitet, um den Zugang zu den verschiedenen Dienstgebäuden und Parkflächen des EPA effizient und effektiv zu verwalten.

Das Kartenverwaltungssystem dient zu folgenden Zwecken:

1. Verwaltung von Ausweisen, um EPA-Bediensteten, Familienangehörigen, Verwaltungsratsmitgliedern, Patentanwälten, Auftragnehmern, EPA-Pensionären, Dienstleistern und Besuchern des EPA Zutritt zu den Gebäuden zu gewähren
2. Überprüfung, ob die Besucher auf der Hausverbotsliste stehen und ob ihnen Zutritt zu den EPA-Gebäuden gewährt werden kann, bevor ein Besucherausweis ausgestellt wird

Überprüfung der Identität der Personen, die einen EPA-Zugangsausweis erhalten, mithilfe automatisierter Identitätsscanner, die gleichzeitig die Echtheit des gescannten Ausweisdokuments überprüfen

Die Verarbeitung personenbezogener Daten im Zugangskontrollsystem dient dazu, den Zugang zu den verschiedenen Dienstgebäuden und Parkflächen des EPA effizient und effektiv zu verwalten.

Das Zugangskontrollsystem dient außerdem dazu, die Einhaltung der einschlägigen Vorschriften (Hausordnung und Rundschreiben zum Thema Sicherheit) zu überwachen sowie zu folgenden Zwecken:

- 1.- EPA-Bediensteten sowie Besuchern und Auftragnehmern einschließlich Dienstleistern Zutritt zu den EPA-Gebäuden zu gewähren
- 2.- die Zugangsprotokolle der Bereiche zu registrieren, zu denen Nutzer Zugang erhalten haben
- 3.- im Fall von Bediensteten, Auftragnehmern und Besuchern, die Zugang zum EPA-Gelände haben, das Kfz-Kennzeichen (bei Ankunft des Fahrzeugs an der Einfahrt) automatisch zu registrieren, um
 - a) die Parkplatznutzung zu überwachen und die Intervention des Verwaltungspersonals bei der Registrierung langfristiger Parkplatzanfragen zu beschränken;
 - b) Bedienstete automatisch zu informieren, wenn sie gegen die Parkordnung verstoßen und ihr Fahrzeug länger als zulässig abstellen (z. B. werden an Bedienstete, die die Parkordnung nicht einhalten, automatisierte E-Mails versandt);
 - c) die verfügbaren Parkmöglichkeiten effizienter zu verwalten (ein Fahrzeug pro Mitarbeiter).

Im Zusammenhang mit dem vorstehend unter Nr. 3 genannten Verarbeitungszweck werden die Kennzeichen von sich der Einfahrt nähernden Fahrzeugen registriert und mit dem entsprechenden Zugangsausweis

verknüpft, um den Fahrzeughalter zu identifizieren und die Parkplatznutzung überwachen zu können (ein Fahrzeug pro Person, maximal zulässige Parkdauer von einem Tag).

4.- Alarm über das Sicherheitsmanagementsystem auszulösen - einschließlich Alarm bei zu lang geöffneter Tür, erzwungenem Öffnen einer Eingangs- oder einer Umgehungstür und Verwendung eines ungültigen Ausweises am Eingang

2. Welche personenbezogenen Daten verarbeiten wir?

Die folgenden Kategorien von personenbezogenen Daten können im Hinblick auf EPA-Bedienstete, die Mitarbeiter von Vertragsfirmen, EPA-Pensionäre, Patentanwälte und Mitglieder des Verwaltungsrats des EPA verarbeitet werden: Vorname, Nachname, Ausweisnummer, Gebäudenummer, Kartengültigkeit, Vertragsbeginn und -ende, Telefonnummer, Zugangscode, Abteilung, E-Mail-Adresse, Mitarbeitergruppe und -untergruppe, Geschlecht, Ausweisnummer, Kommunikationssprache, Dienort, Preisliste für Ermäßigungen und technische Details zu standardmäßigen Kartenverwaltungssystemen.

Die folgenden Kategorien von personenbezogenen Daten können im Hinblick auf Besucher verarbeitet werden: Vorname, Nachname, Geburtsdatum und/oder Nummer des Ausweisdokuments, Ansprechperson im EPA sowie die Zeitstempel mit dem Zeitpunkt des Zutritts zum Gebäude.

Im Hinblick auf Familienangehörige von EPA-Bediensteten (in FIPS registrierte Partner und unterhaltsberechtigter Kinder von EPA-Bediensteten über 16 Jahren) dient die Verarbeitung personenbezogener Daten dazu, diesen Personen einen Familienausweis für den Zugang zu den Sporträumen und halböffentlichen Bereichen des EPA auszustellen, sofern der betreffende Bedienstete dies über MyFIPS beantragt hat. Auf dem Ausweis ist ein Foto des Familienangehörigen abgebildet; außerdem sind der vollständige Name und der EPA-Bedienstete angegeben, um dessen Familienangehörigen es sich handelt.

Alle in einem Reisedokument (Reisepass oder Personalausweis) enthaltenen Datenkategorien werden verarbeitet, aber nicht gespeichert. Sie werden nur während der Identitätsüberprüfung durch Identitätsdokumentscanner verarbeitet und verworfen, sobald das Überprüfungsergebnis vorliegt.

Kennzeichen der Fahrzeuge von Bediensteten und Auftragnehmern, die Zugang zu den Parkflächen des EPA haben, sowie Zeitstempel, wann der Zugang zu den Parkflächen des jeweiligen Gebäudes erfolgt ist. Alle im Verarbeitungsverzeichnis zum Kartenverwaltungssystem aufgeführten Datenkategorien (einschließlich Fotos von Bediensteten und Auftragnehmern für die Zwecke der Zugangskontrolle).

Betroffene Personengruppen bzw. Einzelpersonen:

- ✓ EPA-Bedienstete
- ✓ Familienangehörige von EPA-Bediensteten (über sechzehn Jahre)
- ✓ EPA-Pensionäre
- ✓ Besucher (z. B. Kantinenbesucher, externe Personen)
- ✓ Mitarbeiter von Vertragsfirmen
- ✓ Bedienstete des DPMA Berlin
- ✓ Patentanwälte
- ✓ Verwaltungsratsmitglieder

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung der GD 4 - HD 44 - Allgemeine Verwaltung (vertreten durch den Referatsleiter Facility Management des jeweiligen EPA-Dienstorts) verarbeitet, die als delegierter Datenverantwortliche des EPA handelt.

Personenbezogene Daten werden von den EPA-Bediensteten verarbeitet, die an der jeweiligen Initiative bzw. am jeweiligen Projekt, an der jeweiligen Tätigkeit des Sicherheitsdienstes im Bereich Facility Management beteiligt sind.

Externe Auftragnehmer im Sicherheitsdienst des Bereichs Facility Management, die an dieser Tätigkeit 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?

Die in der GD 4 - HD 44 - Allgemeine Verwaltung tätigen EPA-Bediensteten und erforderlichenfalls die für die Verwaltung der Auftragnehmer zuständigen Vertragsmanager können bedarfsorientiert Zugriff erhalten.

Personenbezogene Daten können zum Zwecke der Bereitstellung von Wartungs- oder Unterstützungsleistungen für Drittanbieter offengelegt werden.

Personenbezogene Daten werden nur an bevollmächtigte Personen weitergegeben, die für die entsprechende Verarbeitung verantwortlich sind, und nicht für andere Zwecke verwendet und auch nicht für andere Empfänger offengelegt.

Werden durch andere Empfänger (z. B. D. 0.4.4 Ethik und Compliance, die Polizei, ein Sicherheitsexperte) Informationen angefordert, so werden diese fallbasiert beim delegierten Datenverantwortlichen angefragt, und das DPO wird konsultiert.

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.

Es 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 von Systemen, Geräten und Netzwerk
- physischer Schutz: EPA-Zugangskontrollen, weitere Zugangskontrollen für das Rechenzentrum, Regeln für das Abschließen von Büros
- Übertragungs- und Eingabekontrollen (z. B. Audit-Protokollierung, System- und Netzwerküberwachung)
- Reaktion auf sicherheitsrelevante Vorfälle: Rund-um-die-Uhr-Überwachung auf Vorfälle, Sicherheitsexperte in Bereitschaft

Auf die in den Zugriffsprotokollen gespeicherten Daten haben nur die Administratoren der Anwendung Zugriff. Der Zugriff auf die Daten erfolgt nur auf Anfrage sowie mit Genehmigung des Verantwortlichen und nach Befürwortung durch das DPO, außer in besonders dringlichen Fällen, in denen das DPO unterrichtet wird. Andere Nutzer mit Zugriff auf die Daten, z. B. der externe Sicherheitsdienstleister, haben nur Zugriff auf die Daten, die zum Zwecke der Registrierung des Zugangs zu den EPA-Gebäuden gespeichert sind.

Der Zugriff auf die Anwendung und die darin gespeicherten Daten wird bedarfsorientiert gewährt. Administratoren des EPA-Sicherheitsdiensts haben zur Überwachung der Einhaltung der Vorschriften Zugriff auf gespeicherte Protokolldateien, und der externe Sicherheitsdienstleister hat für den Betrieb der Anwendung eingeschränkten Zugriff.

Der Zugriff auf die Anwendung erfordert die Authentifizierung über BIT-Tools (Passwort/Active Directory) sowie ein zusätzliches Passwort für die Anwendung. Die personenbezogene Daten verarbeitenden Auftragnehmer haben sich in einer rechtsverbindlichen Vereinbarung verpflichtet, die sich aus dem anwendbaren Datenschutzrahmen ergebenden Verpflichtungen zu erfüllen.

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

Sie haben gemäß den Artikeln 18 bis 24 der Datenschutzvorschriften des EPA das Recht, auf Ihre personenbezogenen Daten zuzugreifen, sie zu berichtigen, sie zu erhalten, sie löschen zu lassen sowie die Verarbeitung Ihrer Daten zu beschränken und ihr zu widersprechen.

Wenn Sie von einem dieser Rechte Gebrauch machen möchten, wenden Sie sich als externer Nutzer bitte schriftlich an DPOexternalusers@epo.org oder ansonsten an den delegierten Datenverantwortlichen unter DPL.PD44@epo.org. 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 Amts notwendige Verarbeitung einschließt, erforderlich" (Gewährleistung der Gebäudesicherheit).

Personenbezogene Daten werden im Einklang mit folgendem Rechtsakt erhoben und verarbeitet:

Betreffend die dem EPA übertragenen Aufgaben (Rundschreiben Nr. 380, Art. 2 e)): Der Sicherheitsdienst gewährleistet die Einhaltung der Hausordnung, den ungehinderten Dienstbetrieb des EPA und die Beachtung der geltenden Gesetze und Vorschriften. Er ist befugt, alle hierfür erforderlichen Anweisungen zu geben und Maßnahmen zu treffen. Insbesondere kann er hierfür Identitäts- und Sicherheitskontrollen durchführen.

Die oben erläuterten Gründe werden als zielgerichtetes und verhältnismäßiges Mittel erachtet, die Sicherheit der in den Gebäuden arbeitenden Belegschaft zu gewährleisten, wenn der Sicherheitsdienst für die Bereitstellung der erforderlichen Notfallmaßnahmen verantwortlich ist, und das angemessene Maß an Sicherheit für die vertraulichen Informationen und die Vermögenswerte des EPA aufrechtzuerhalten - und zu diesem Zweck die Sicherheitssysteme so zu nutzen, dass Notfallmaßnahmen effizient erfolgen können.

8. Wie lange speichern wir Ihre Daten?

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

Im Zugangskontrollsystem (ACS) werden Zugangsprotokolle, die älter als 12 Monate sind, durch eine in der Software programmierte automatisierte Routine überschrieben.

Besucherdaten werden im Einklang mit den Verzeichnissen zur Videoüberwachung und zu Sicherheitszwecken nur für 28 Tage aufbewahrt. Dies ermöglicht den Sicherheitskräften im Fall der Anzeige von Straftaten die Durchführung unterstützender Ermittlungen betreffend den Zutritt von Besuchern.

Für das Kartenverwaltungssystem (CMS) werden Daten aus FIPS gemäß der für FIPS festgelegten Aufbewahrungsdauer gespeichert und gelöscht (bei Löschung in FIPS werden jegliche Daten von Bediensteten oder Auftragnehmern gelöscht).

Für Gruppen wie den Verwaltungsrat oder Patentanwälte, die der sogenannte Datenmanager manuell hinzufügt, führt dieser mindestens einmal pro Jahr oder bei jeder Meldung einer Änderung eine Konformitätskontrolle durch. Dabei überprüft der Datenmanager die Daten auf Gültigkeit und Richtigkeit und nimmt alle erforderlichen Änderungen und/oder Löschungen vor, um die Daten auf dem neuesten Stand zu halten.

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

9. Kontaktinformationen

Bei Fragen zur Verarbeitung Ihrer personenbezogenen Daten wenden Sie sich als externer Nutzer bitte an das Datenschutzbüro und/oder den delegierten Datenverantwortlichen unter DPOexternalusers@epo.org. EPA-Bedienstete wenden sich bitte an den delegierten Datenverantwortlichen unter DPL.PD44@epo.org.

Unsere Datenschutzbeauftragte erreichen Sie unter dpo@epo.org.

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.