Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen des Identitätsmanagements durch Active Directory und Azur Active Directory

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 bezieht sich auf die Bereitstellung von Nutzerkonten und diesbezüglichen Zugriffsregeln und Zuweisungen durch die Verwendung von Active Directory (AD) und Azure AD als zentrales Archiv für Benutzeridentitäten.
Das EPA verwendet AD und Azure AD für die Zwecke des Identitäts- und Zugriffsmanagements.

Derzeit gibt es zwei Szenarien für die Bereitstellung von Nutzerkonten:

1. Interne Nutzer (Beschäftigte und Auftragnehmer) werden in FIPS (Master) definiert, das mit On Premise AD synchronisiert wird. Danach wird On Premise AD mit Azure AD synchronisiert.

2. Nutzer in nationalen Patentämtern: Als Master-Quelle fungiert das Einheitliche Zugangsportal, in dem Nutzer erstellt, aktualisiert und gelöscht werden. Das Einheitliche Zugangsportal wird mit On Premise AD synchronisiert. Danach wird On Premise AD mit Azure AD synchronisiert.

Nutzerkonten werden anschließend für Authentifizierungs- und Autorisierungszwecke verwendet.

Das EPA verarbeitet die Daten nicht zur Verwendung für eine automatisierte Entscheidungsfindung (einschließlich Profiling).

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, wird 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?

Verarbeitete personenbezogene Daten, wenn die betroffene Person EPA-Bediensteter oder Auftragnehmer des EPA ist:

- Persönliche Identifikationsdaten: Vorname, Nachname, Geschlecht, Foto, bevorzugte Kommunikationssprache, digitale Signatur, digitales Zertifikat
- Kontaktinformationen: E-Mail-Adresse (geschäftlich), Telefonnummern, Mobiltelefonnummer

- Angaben zum Nutzerkonto: Personalnummer, Benutzer-ID, Konto-ID, Kontoalter, Kontokennwort, Kennwort-Hash, Zeitpunkt der letzten Anmeldung, Mitgliedschafts- und Eigentumsberechtigungen
- Browsing-Informationen: Browser-Typ, User-Agent des Browsers, Browsing-Datum und Uhrzeit, Browsing-Dauer
- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsmetadaten, Sitzungsdetails, IP-Adresse
- Systemprotokolle: system-, anwendungs- und sicherheitsbezogene Serverprotokolle
- Geräteverwaltungsdaten: Windows-ID für Windows-Geräte, Mieter-ID, Geräte-ID Azure Active Director
- Arbeitsplatzinformationen: Abteilungsname und/oder -nummer, Unternehmensbereich, Personalnummer, Indikator "aktiv/inaktiv", Vorgesetzter, Zimmernummer, Stellenbezeichnung, Bürostandort, Unternehmenseinheit (nur für Auftragnehmer)
- Physische und/oder digitale Ressourcen: Hostname der Workstation (physisch oder virtuell), Kennung des Videokonferenzraums/der Ausrüstung (nur für Bedienstete), Name des mobilen Geräts, Version des Betriebssystems
- Gebäudebereich und Standort

Verarbeitete personenbezogene Daten, wenn die betroffene Person eine externe Person ist:

- Persönliche Identifikationsdaten: Vorname, Nachname, Land
- Kontaktinformationen: E-Mail-Adresse (geschäftlich), Telefonnummern
- Angaben zum Nutzerkonto: Kontonummer, Kontoalter, Kontopasswort, Passwort-Hash, Mitglieds- und Nutzerberechtigungen
- Browsing-Informationen: Browser-Typ, Browsing-Dauer
- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsmetadaten, Sitzungsdetails, IP-Adresse
- Systemprotokolle: system-, anwendungs- und sicherheitsbezogene Serverprotokolle
- Beschäftigungsangaben: Unternehmenseinheit

Verarbeitete personenbezogene Daten, wenn die betroffene Person eine externe Person ist:

- Persönliche Identifikationsdaten: Vorname, Nachname
- Angaben zum Nutzerkonto: Nutzer-ID, Kontoalter, Kontopasswort, Passwort-Hash, Mitgliedschaftsberechtigungen
- Browsing-Informationen: Browser-Typ, Browsing-Dauer
- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsmetadaten, Sitzungsdetails, IP-Adresse
- Systemprotokolle: system-, anwendungs- und sicherheitsbezogene Serverprotokolle

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung des Chief Information Officer (BIT, HD 4.6) verarbeitet,
der als delegierter Datenverantwortlicher des EPA handelt.

Personenbezogene Daten werden auch von Bediensteten der HD 4.6 verarbeitet, die an der Verwaltung der in dieser Erklärung benannten Anwendungen beteiligt sind.

Externe Auftragnehmer, die an Aufgaben hinsichtlich des Identitäts- und Zugriffsmanagements beteiligt sind, dürfen ebenfalls personenbezogene Daten verarbeiten und ggf. darauf zugreifen.

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

Personenbezogene Daten werden bedarfsorientiert wie folgt offengelegt für:

- EPA-Bedienstete und Auftragnehmer (Systemadministratoren) der Abteilung Informationssicherheit 4.6.2.3
- EPA-Personal insgesamt: Lesezugriff (direkt über den Browser), z. B. über das Telefonbuch oder indirekt über APIs zu anderen Microsoft-Anwendungen (z. B. Outlook, MS-Teams usw.) im Hinblick auf personenbezogene Daten anderer EPA-Bediensteter
- auf personenbezogene Daten in AD/Azure AD wird von EPA-Anwendungen zum Zwecke der Nutzerauthentifizierung/-Autorisierung zugegriffen

Personenbezogene Daten können für Dritte zum Zwecke der Datenpflege, Unterstützung und Sicherung offengelegt werden.

Personenbezogene Daten werden nur an entsprechend befugte Personen weitergegeben, die für die notwendigen Verarbeitungsvorgänge zuständig sind, und weder für andere Zwecke verwendet noch 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 Identitätsmanagementsysteme, die in den Räumlichkeiten des EPA gehostet werden, gelten die folgenden Sicherheitsmaßnahmen:
Alle mit dem Identitätsmanagement zusammenhängenden personenbezogenen Daten werden in sicheren IAM-Anwendungen gemäß den Sicherheitsstandards des EPA gespeichert. Zu diesen Diensten gehören:

- Nutzerauthentifizierung: Alle Workstations und Server benötigen eine Anmeldung, mobile Geräte benötigen eine Anmeldung für den EPA-internen Bereich, privilegierte Konten benötigen eine zusätzliche und strengere Authentifizierung.
- Zugriffskontrolle (z. B. rollenabhängige Zugriffskontrolle auf die Systeme und das Netzwerk, Bedarfsorientiertheit und Least-Privilege-Prinzip): Trennung in Administrator- und Nutzerrollen, Nutzer haben eine minimale Berechtigung, allgemeine Administratorrollen werden auf ein Minimum beschränkt
- Virenschutz auf allen Geräten
- Physischer Schutz: EPA-Zugangskontrollen, zusätzliche Zugangskontrollen zum Rechenzentrum
- Übertragungs- und Eingabekontrollen: Audit-Protokollierung, System- und Netzwerküberwachung, Sicherheitsüberwachung
- Reaktion auf Sicherheitsvorfälle: Rund-um-die-Uhr-Überwachung auf Vorfälle, Sicherheitsexperte in Bereitschaft

Für personenbezogene Daten, die auf nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, haben die die personenbezogenen Daten verarbeitenden Provider in einer bindenden Vereinbarung zugesagt, die sich aus dem anwendbaren Datenschutzrahmen ergebenden Verpflichtungen zu erfüllen. Das EPA hat außerdem eine Überprüfung der Datenschutz- und Sicherheitsrisiken durchgeführt. Diese Anbieter müssen geeignete technische und organisatorische Maßnahmen umgesetzt haben, wie z. B.: physische Sicherheitsmaßnahmen, Zugriffs- und Speicherkontrollmaßnahmen, Sicherung von ruhenden Daten (z. B. mittels 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).

Azure AD ist nach verschiedenen Sicherheitsstandards zertifiziert (z. B. SOC 1 Typ II, SOC 2 Typ II).

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 als betroffene Person 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 den delegierten Datenverantwortlichen unter DPOexternalusers@epo.org oder andernfalls als interner Nutzer an den delegierten Datenverantwortlichen unter DP_BIT@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, als interner Nutzer dieses Formular und/oder als Ruhegehaltsempfänger dieses Formular auszufüllen und zusammen mit Ihrem Antrag einzureichen.

Wir werden Ihren Antrag baldmöglichst und in jedem Fall innerhalb eines Monats nach Eingang 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?
Wir verarbeiten personenbezogene Daten gemäß Artikel 5 a) DSV: 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.

Nutzerdaten werden so lange aufbewahrt, bis sie im Master-(Quell-)System (d. h. in FIPS oder im Einheitlichen Zugangsportal) als inaktiv markiert werden, und bewahren sie dann für weitere 30 Tage sowohl in On Premise AD als auch in Azure AD auf.

Während der Laufzeit des Abonnements hat das EPA jederzeit die Möglichkeit, auf die in den Anwendungen gespeicherten Daten im Rahmen dieses Datensatzes zuzugreifen, diese zu extrahieren und zu löschen. Microsoft wird EPA-Daten, die in den Anwendungen gespeichert bleiben, 90 Tage lang nach Ablauf oder Beendigung des Abonnements des EPA in einem eingeschränkten Funktionskonto aufbewahren, damit das EPA die Daten extrahieren kann.

Nach Ablauf der 90-tägigen Aufbewahrungsfrist deaktiviert Microsoft das Konto des EPA und löscht die EPA-Daten und personenbezogenen Daten innerhalb weiterer 90 Tage, es sei denn, Microsoft ist gemäß dem Vertrag mit dem EPA zur Aufbewahrung dieser Daten berechtigt.

Microsoft löscht alle Kopien von personenbezogenen Daten in Verbindung mit den Anwendungen im Rahmen dieses Datensatzes, nachdem die geschäftlichen Zwecke erfüllt wurden, zu denen die Daten erhoben oder übermittelt wurden (auf Wunsch des EPA auch früher), es sei denn, Microsoft ist gemäß dem Vertrag mit dem EPA zur Aufbewahrung dieser Daten berechtigt. 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 sich externe betroffene Personen unter DPOexternalusers@epo.org an den Datenschutzbeauftragten und/oder den delegierten Datenverantwortlichen.

EPA-Bedienstete wenden sich bitte an den delegierten Datenverantwortlichen unter DP_BIT@epo.org oder an den Datenschutzbeauftragten 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.