Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Verwendung von E-Mails beim Europäischen Patentamt

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 personenbezogenen Daten, anhand deren Sie direkt oder indirekt identifizierbar sind, werden auf rechtmäßige Weise, nach Treu und Glauben 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 der Datenschutzvorschriften des EPA (DSV) mitgeteilt.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Diese Datenschutzerklärung bezieht sich auf die Verarbeitung personenbezogener Daten im Zusammenhang mit den E-Mail- und Kalenderanwendungen, die den EPA-Mitarbeitern zur Verfügung stehen: Für die Verarbeitung werden Microsoft Exchange Online und Microsoft Outlook verwendet. Outlook umfasst auch nicht optionale verbundene Erfahrungen, die eine effizientere Inhaltserstellung, Kommunikation und Zusammenarbeit ermöglichen sollen.

Die Erfassung personenbezogener Daten erfolgt zu folgenden Zwecken:

- um die Kommunikation in Form von E-Mail-Nachrichten, Anhängen und Kalenderaktionen zwischen EPA-Bediensteten und externen Nutzern über Nutzer-Clients und APIs (Application Program Interfaces) zu ermöglichen;
- um den Nutzern des EPA-E-Mail-Systems ein Adressbuch zur Verfügung zu stellen, dem Adressen, Mailinglisten und Gruppen von EPA-Empfängern zu entnehmen sind;
- um den E-Mail-Verkehr zum Zwecke der IT-Problembehebung und Cybersicherheit nachverfolgen zu können;
- um einen Sicherungsmechanismus bereitzustellen, mit dem die Nutzer des EPA-E-Mail-Systems E-Mail-Nachrichten wiederherstellen können, die sie zuvor versehentlich gelöscht haben.

Die verarbeiteten Daten werden nicht für automatisierte Entscheidungen einschließlich Profiling verwendet.

Ihre personenbezogenen Daten werden nicht an Empfänger außerhalb des EPA übermittelt, die nicht unter Artikel 8 Absätze 1, 2 und 5 DSV fallen, sofern kein angemessenes Schutzniveau gewährleistet ist. Falls kein angemessenes Schutzniveau besteht, darf die Übermittlung nur erfolgen, sofern geeignete Garantien vorgesehen sind und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen oder wenn Ausnahmen für bestimmte Fälle gemäß Artikel 10 DSV gelten. Im Rahmen der Nutzung von Microsoft Outlook und Exchange Online können Übermittlungen zu folgenden begrenzten Zwecken erfolgen: Schutz vor Schadsoftware, Anmeldung bei Azure Active Directory, Lastverteilung, Diagnosedaten, verbundene Erfahrungen und Verarbeitung für die Geschäftsaktivitäten von Microsoft.

2. Welche personenbezogenen Daten verarbeiten wir?

Die folgenden Kategorien und Arten personenbezogener Daten können im Zusammenhang mit der Verwendung von E-Mails verarbeitet werden:

Wenn die betroffene Person EPA-Bediensteter ist:

- Angaben zur persönlichen Identifizierung: Vorname, Nachname, digitale Signatur;
- Kontaktinformationen: geschäftliche E-Mail-Adresse, Telefonnummern, Kontaktdaten;
- beschäftigungsbezogene Angaben: Standort, Abteilungsname und/oder -nummer, Stellenbezeichnung/Funktion, Zimmernummer, Bürostandort, Vorgesetzter (nur für interne Bedienstete);
- Angaben zum Nutzerkonto: Nutzerkennung, Nutzerberechtigungen, Mitgliedsberechtigungen;
- physische und/oder identifizierbare digitale Assets: Hostname der Workstation, Betriebssystemversion, digitales Zertifikat (nur bestimmte Bedienstete), Videokonferenzraum/Geräte-ID;
- Netzwerk-/Anwendungsinteraktionsdaten: Sitzungsmetadaten, Sitzungsinhalt, Sitzungsdetails;
- Browsing-Informationen: Browser-Typ, User-Agent des Browsers, Cookie-Informationen, URL, Datum und Uhrzeit von Browsing-Sitzungen, IP-Adresse, Netzwerkinteraktionsverlauf;
- sensorische und elektronische Informationen: Anwesenheitsstatus;
- Systemprotokolle: Dateidaten (Name, Größe und/oder Hash), system-/anwendungs-/sicherheitsbezogene Serverprotokolle, Prüfprotokolle, Transaktionsdetails;
- personenbezogene Informationen, die die betroffene Person im Rahmen des E-Mail-Versands für berufliche Tätigkeiten freiwillig bereitstellt (z. B. Nachrichten, Bilder, Dateien, Sprachnachrichten, Kalendereinträge für Besprechungen, Kontakte u. Ä.) sowie zusätzliche Informationen, die im Laufe des E-Mail-Kommunikationsaustauschs eventuell ohne Eingreifen des Absenders bereitgestellt werden (wenn ein Absender z. B. eine E-Mail über einen Internetbrowser sendet, kann die sendende Engine die IP-Adresse des Browsers zu einem der SMTP-Header der Nachricht hinzufügen).

Wenn die betroffene Person ein externer Nutzer ist:

- Angaben zur persönlichen Identifizierung: Vorname, Nachname, digitale Signatur;
- Kontaktinformationen: private E-Mail-Adresse, berufliche E-Mail-Adresse;
- Netzwerk-/Anwendungsinteraktionsdaten: Sitzungsmetadaten, Sitzungsinhalt, Sitzungsdetails;
- Browsing-Informationen: IP-Adresse, Datum und Uhrzeit von Browsing-Sitzungen, Netzwerkinteraktionsverlauf;
- Systemprotokolle: Transaktionsdetails, system-/anwendungs-/sicherheitsbezogene Serverprotokolle, Dateidaten (Name, Größe und/oder Hash);
- personenbezogene Informationen, die die betroffene Person im Rahmen des E-Mail-Versands für berufliche Tätigkeiten freiwillig bereitstellt (z. B. Nachrichten, Bilder, Dateien, Sprachnachrichten, Kalendereinträge für Besprechungen, Kontakte u. Ä.) sowie zusätzliche Informationen, die im Laufe des E-Mail-Kommunikationsaustauschs eventuell ohne Eingreifen des Absenders bereitgestellt werden (wenn die betroffene Person z. B. eine E-Mail über einen Internetbrowser sendet, kann die sendende Engine die IP-Adresse des Browsers zu einem der SMTP-Header der Nachricht hinzufügen).

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Die Verarbeitung personenbezogener Daten erfolgt unter der Verantwortung des Chief Information Officers des EPA (HD 4.6) in seiner Funktion als delegierter Datenverantwortlicher des EPA.

Personenbezogene Daten werden von den Bediensteten von HD 4.6 zum Zwecke der Bereitstellung, des Betriebs, des Supports und der Wartung von Microsoft Exchange Online und Outlook verarbeitet.

Externe Anbieter, die mit dem Support, dem Betrieb und der Wartung von Outlook und Exchange Online befasst sind – u. a. Microsoft – können ebenfalls auf personenbezogene Daten zugreifen und diese verarbeiten.

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

Personenbezogene Daten werden bedarfsorientiert offengelegt gegenüber:

- Empfängern einzelner E-Mails und/oder einzelner Kalendereinträge (potenziell allen Nutzern);
- Empfängern in BIT PACE 4615 zum Zwecke der Administration, des Betriebs und der Wartung des E-Mail-Systems; Empfängern in BIT Security 4623 für die Zwecke der Cybersicherheit von E-Mails;
- Microsoft-Mitarbeitern und EPA-Bediensteten in HD 4.6, deren Aufgabe in Bereitstellung und Administration sowie Betrieb und Wartung des E-Mail-Dienstes besteht;
- allen Nutzern von E-Mails beim EPA (Bediensteten oder Auftragnehmern), die Lesezugriff auf die Informationen im Outlook-Adressbuch des EPA haben.

In Microsoft 365 (Anwendungssuite, die auch Exchange Online und Outlook umfasst) ist grundsätzlich der überwiegende Teil des Servicebetriebs automatisiert, um die Notwendigkeit eines menschlichen Zugriffs zu verringern. Jeder erforderliche Zugriff ist zeitlich begrenzt und erfolgt mit eingeschränkten Zugriffsrechten.

5. Wie schützen wir Ihre personenbezogenen Daten?

Wir ergreifen angemessene technische und organisatorische Maßnahmen, um Ihre personenbezogenen Daten vor Vernichtung, Verlust oder Veränderung in unbeabsichtigter oder unrechtmäßiger Weise sowie unbefugter Offenlegung oder unbefugtem Zugang zu schützen.

Für personenbezogene Daten, die auf nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, haben die Anbieter, die die personenbezogenen Daten verarbeiten, 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.

Personenbezogene Daten, die über öffentliche Netzwerke zwischen dem EPA und Microsoft oder zwischen Microsoft-Rechenzentren übertragen werden, werden standardmäßig verschlüsselt. Personenbezogene Daten, die Bestandteil der vom oder im Auftrag des EPA durch die Nutzung von Microsoft-365-Diensten an Microsoft übermittelten Daten sind, werden im Ruhezustand verschlüsselt. Für die Verschlüsselung setzt Microsoft Verschlüsselungstechnologien nach dem neuesten Stand der Technik ein. Des Weiteren nutzt Microsoft Zugriffsmechanismen, die auf dem Grundsatz der geringsten Berechtigung beruhen, um den Zugriff auf personenbezogene Daten, die Bestandteil der vom EPA an Microsoft übermittelten Daten sind, zu kontrollieren, und setzt eine rollenbasierte Zugriffssteuerung ein, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf solche personenbezogenen Daten einem angemessenen Zweck dient und unter Aufsicht des Vorgesetzten genehmigt ist. Bei Microsoft-365-Anwendungen ist jeder erforderliche Zugriff durch Microsoft zeitlich begrenzt.

Bei Microsoft-365-Anwendungen erfolgt die Implementierung und Aufrechterhaltung verschiedener Sicherheitsmaßnahmen zum Schutz personenbezogener Daten, die Bestandteil der vom EPA durch die Nutzung von Microsoft-365-Diensten an Microsoft übermittelten Daten sind, darunter: Organisation der IT-Sicherheit (z. B. Verantwortung für die Sicherheit, Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit, Risikomanagementprogramm), Asset-Management (z. B. Führen eines Anlagenbestands und Asset-Handling), Personalsicherheit (z. B. Sicherheitsschulungen), physische und umgebungsbezogene Sicherheit (z. B. physischer Zugang zu Einrichtungen, physischer Zugriff auf Komponenten, Schutz vor Unterbrechungen, Entsorgung von Komponenten), Kommunikations- und Betriebsmanagement (z. B. Betriebsrichtlinie, Datenwiederherstellungsverfahren, Anti-Schadsoftware-Kontrollen,

Ereignisprotokollierung), Zugriffskontrolle (z. B. Zugriffsrichtlinie, Zugriffsberechtigung, geringste Rechte, Integrität und Vertraulichkeit, Authentifizierung, Netzwerkdesign), Handhabung eines Informationssicherheitsvorfalls (z. B. Vorfallreaktionsablauf, Dienstüberwachung) und Geschäftsfortführungsmanagement. Microsoft ergreift auch geeignete technische und organisatorische Maßnahmen zum Schutz etwaiger weiterer personenbezogener Daten, die sich von den oben beschriebenen unterscheiden, und legt diese Maßnahmen in einer Microsoft-Sicherheitsrichtlinie fest.

Microsoft-365-Anwendungen sind so konfiguriert, dass die Vertraulichkeit der Informationen durch die Ergreifung der oben aufgeführten Maßnahmen gewahrt wird. Des Weiteren ist ein anonymer Zugriff nicht gestattet. Jegliche Informationen, die per Chat, Videokonferenz oder Dateifreigabe in Microsoft 365 aufgenommen werden, stehen ausschließlich den in Abschnitt 4 angegebenen speziellen Nutzern und Gruppen zur Verfügung.

Microsoft-365-Anwendungen sind nach mehreren Sicherheitsstandards zertifiziert, darunter ISO 27001, SOC 1 Typ II, SOC 2 Typ II sowie ISO 27018 "Leitfaden zum Schutz personenbezogener Daten in öffentlichen Cloud-Diensten", und sie entsprechen den Anforderungen gemäß ISO 27002.

Microsoft führt jährliche Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren durch, die Microsoft zur Verarbeitung personenbezogener Daten nutzt. Die Prüfungen werden von unabhängigen dritten Prüfern entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder bestimmungen durchgeführt.

Personenbezogene Daten werden gemäß der vom EPA vorgenommenen Anwendungskonfiguration in der EU gespeichert. Sie können jedoch abhängig von den Anforderungen an Wartung, Support und Betrieb für die cloudgehosteten Dienste und der Verfügbarkeit dieses Fachwissens Unterauftragsverarbeitern in anderen Ländern zur Verfügung gestellt werden. Die Gewährung eines Zugriffs ist stets zeitlich begrenzt und erstreckt sich nur auf die Daten, die für den jeweils ausgeführten Wartungs-, Support- oder Betriebsvorgang erforderlich sind. Die folgenden Schutzvorkehrungen werden getroffen:

• bei allen Übertragungen an Drittländer verwendet Microsoft EU-Standardvertragsklauseln für die Datenübertragung an seine Unterauftragsverarbeiter;
• Microsoft verlangt von den Unterauftragsverarbeitern, dass sie dem Microsoft Supplier Security and Privacy Assurance Program beitreten. Dieses Programm dient der Standardisierung und Verbesserung der Datenverarbeitungsverfahren und soll sicherstellen, dass die Geschäftsprozesse und -systeme der Lieferanten mit denjenigen von Microsoft in Einklang stehen.

EPA-spezifische Maßnahmen in Verbindung mit Exchange Online und Outlook:

- für den Zugriff auf das E-Mail-Postfach sind EPA-Anmeldedaten nach aktuellen Authentifizierungsstandards erforderlich;
- der Zugriff mittels Geräten, die nicht Bestandteil der Domäne sind, unterliegt der Multi-Faktor-Authentifizierung (MFA);
- Authentifizierung und Autorisierung basieren auf Rollen; bei der Aktivierung von Rollen wird ebenfalls MFA erzwungen;
- es erfolgen Zugriffsprüfungen anhand vorhandener Rollen; es gibt einen Audit-Verlauf.

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

Sie haben das Recht, auf Ihre personenbezogenen Daten zuzugreifen, sie zu berichtigen und sie abzurufen, 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 bitte schriftlich unter DP_BIT@epo.org an den delegierten Datenverantwortlichen. Externe Nutzer sollten sich unter DPOexternalusers@epo.org an den Datenschutzbeauftragten und/oder den delegierten Datenverantwortlichen wenden. Damit wir schneller und genauer darauf antworten können, brauchen wir stets bestimmte Vorabinformationen. Deshalb bitten wir externe Nutzer dieses Formular und interne 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 Absatz 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 Buchstabe 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."

Um die Anforderungen an die Cybersicherheit zu erfüllen, werden personenbezogene Daten auf der Grundlage des folgenden Rechtsinstruments verarbeitet: Rundschreiben 382 zu Richtlinien für die Informationssicherheit (Artikel 7 "Überwachung, Kontrolle, Auditierung und weitere Verarbeitung").

8. Wie lange speichern wir Ihre Daten?

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

• E-Mail-Informationen und etwaige vom Nutzer des EPA-E-Mail-Systems erstellte persönliche Adressbücher werden so lange gespeichert, wie der Nutzer die Nachricht aufbewahren möchte und er eine vertragliche Verpflichtung gegenüber dem EPA hat.
• Vom Benutzer freiwillig gelöschte E-Mail-Nachrichten werden 90 Tage lang aufbewahrt und dann endgültig gelöscht.
• Die personenbezogenen Daten im globalen Adressbuch und das Postfach eines Nutzers werden so lange gespeichert, wie der Nutzer (z. B. Mitarbeiter, Auftragnehmer) eine vertragliche Verpflichtung gegenüber dem EPA hat. Nach Ablauf des Vertrags des Nutzers werden die Daten noch maximal eineinhalb Jahre (18 Monate) zum Zwecke des Abrufs beim EPA oder einer möglichen Vertragsverlängerung aufbewahrt. Nach Ablauf dieser Frist werden die Daten endgültig gelöscht.
• Im Falle eines Rechtsanspruchs oder einer administrativen Untersuchung, unabhängig davon, ob es sich um ein disziplinarisches oder ein strafrechtliches Vergehen handelt, können personenbezogene Daten länger als die vorstehend genannten Aufbewahrungsfristen aufbewahrt werden. In solchen Fällen, die über den Umfang der delegierten Verantwortlichkeit von BIT HD 4.6 hinausgehen, wird über die Aufbewahrung personenbezogener Daten fallabhängig vom zuständigen delegierten Datenverantwortlichen entschieden.

Des Weiteren hat das EPA während der Laufzeit seines Vertrags mit Microsoft jederzeit die Möglichkeit, auf die in Outlook und Exchange Online gespeicherten Daten zuzugreifen, diese zu extrahieren und zu löschen. Microsoft wird EPA-Daten, die in den Online-Diensten 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, 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 formellen Beschwerde/eines formellen Rechtsstreits werden alle zum Zeitpunkt der Einleitung des formellen Beschwerde-/Rechtsstreitverfahrens gespeicherten Daten bis zum Abschluss des jeweiligen Verfahrens aufbewahrt.

9. Kontaktinformationen

Bei Fragen zur Verarbeitung Ihrer personenbezogenen Daten wenden Sie sich bitte schriftlich an den delegierten Datenverantwortlichen unter DP_BIT@epo.org (EPA-Bedienstete) oder an DPOexternalusers@epo.org (externe betroffene Personen).

Interne Nutzer erreichen den Datenschutzbeauftragten unter dpo@epo.org, externe Nutzer unter DPOexternalusers@epo.org.

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 Verantwortlichen zu stellen, und wenn Sie mit dem Ergebnis der Überprüfung nicht einverstanden sind, haben Sie das Recht, gemäß Artikel 50 DSV Rechtsmittel einzulegen.