Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit Microsoft-365-Anwendungen

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 derer 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 DSV mitgeteilt.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Diese Datenschutzerklärung bezieht sich auf die Verarbeitung personenbezogener Daten im Zusammenhang mit Microsoft-365-Anwendungen, zu denen die folgenden cloudbasierten Anwendungen gehören: OneDrive, SharePoint Online, MS Teams, MS Forms, Word, Excel und PowerPoint. Die in Microsoft 365 beinhalteten Anwendungen sollen den Nutzern eine erhöhte Flexibilität bieten und die Kommunikation und Zusammenarbeit sowohl innerhalb des EPA als auch zwischen dem EPA und externen Stakeholdern verbessern.

Wie oben erwähnt gehört zu den Microsoft-365-Anwendungen auch die Anwendung MS Teams mit den Hauptfunktionen Business Messaging, Telefonie, Audio- und Video-Meetings sowie Dateifreigabe.
MS Teams ist eine cloudbasierte Anwendung für die Organisation von Online-Meetings und Telefonkonferenzen sowohl innerhalb des EPA als auch zwischen dem EPA und externen Stakeholdern. Neben diesen Hauptfunktionen ermöglicht MS Teams die Aufzeichnung von Online-Meetings und die Verwendung von Live-Untertiteln. Die Nutzung solcher Funktionen ist nur bestimmten Stakeholdern gestattet und erfolgt im Einklang mit den EPA-Richtlinien über die Nutzung von MS Teams.

Darüber hinaus umfasst Microsoft 365 auch nicht optionale "verbundene Erfahrungen", die eine effizientere Inhaltserstellung, Kommunikation und Zusammenarbeit ermöglichen sollen.

Die Bediensteten des EPA setzen Microsoft-365-Anwendungen bei der Erfüllung ihrer täglichen Aufgaben ein.

Des Weiteren erfolgt die Verarbeitung personenbezogener Daten zu folgenden vom delegierten Datenverantwortlichen, d. h. dem Chief Information Officer des EPA (Business Information Technology (BIT) – Hauptdirektion (HD) 4.6), festgelegten Zwecken:

• Bereitstellung von Microsoft-365-Anwendungen und -Dienstleistungen gegenüber Bediensteten und Auftragnehmern des EPA.
• Endnutzerunterstützung und Fehlerbeseitigung für Microsoft-365-Anwendungen und -Funktionen.
• Verwaltung von in Microsoft-365-Anwendungen hochgeladenen Inhalten.
• Verwaltung von Microsoft-365-Einstellungen.
• Support, Betrieb und Wartung für Microsoft-365-Anwendungen.

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

Microsoft-Office-365-Anwendungen können für unterschiedliche spezifische Zwecke und Szenarien eingesetzt werden, die in dieser Datenschutzerklärung nicht vollständig beschrieben werden. Die spezifischen

Zwecke und Szenarien, für die Microsoft-365-Anwendungen zur Verarbeitung personenbezogener Daten eingesetzt werden, werden in speziellen Datenschutzerklärungen und einem zugehörigen Verzeichnis von Verarbeitungstätigkeiten beschrieben.

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 der oben aufgeführten Microsoft-Anwendungen 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 in Microsoft-365-Anwendungen verarbeitet werden:

Wenn die betroffene Person EPA-Bediensteter ist:

- Angaben zur persönlichen Identifizierung: Vorname, Nachname, Bild, digitale Signatur
- Kontaktinformationen: geschäftliche E-Mail-Adresse, Telefonnummern
- Beschäftigungsbezogene Angaben: Standort, Abteilungsname und/oder -nummer, Stellenbezeichnung/Funktion, Zimmernummer, Bürostandort, bevorzugte Sprache (für die Kommunikation)
- Angaben zum Nutzerkonto: Nutzerkennung, Nummer des Kontos, Alter des Kontos, Nutzerberechtigungen, Mitgliedsberechtigungen
- Physische und/oder identifizierbare digitale Assets: Name des Mobilgeräts, Rechnername, Betriebssystemversion
- Geräteverwaltungsdaten: letzte Anmeldung, Kontokennung
- Netzwerk-/Anwendungsinteraktionsdaten: Sitzungsmetadaten, Sitzungsinhalt, Sitzungsdetails
- Standortdaten
- Browsing-Informationen: Browser-Typ, User-Agent des Browsers, Verlauf der aufgerufenen Websites, Cookie-Informationen, URL, Datum und Uhrzeit von Browsing-Sitzungen, IP-Adresse, Netzwerkinteraktionsverlauf, Browsing-Dauer
- Sensorische und elektronische Informationen: Anwesenheitsstatus, Audioinformationen, visuelle Informationen
- Telefonie-Interaktionsdaten: Telefonie-Sitzungsmetadaten, Telefonie-Sitzungsinhalt, Telefonie-Sitzungsdetails
- Anrufinformationen: gewählte Rufnummer, Rufnummer des Anrufers, Datum und Uhrzeit von Anrufen, Anrufliste, Anruf-Interaktionsverlauf, Anrufdauer
- Systemprotokolle: Dateidaten (Name, Größe und/oder Hash), Registry-Daten, ausgeführte Prozesse, Portnummern, Webserver-Protokolle, system-/anwendungs-/sicherheitsbezogene Serverprotokolle, Prüfprotokolle, Transaktionsdetails
- Personenbezogene Informationen, die die betroffene Person im Rahmen der Dateifreigabe für berufliche Tätigkeiten freiwillig bereitstellt (z. B. Nachrichten, Bilder, Dateien, Sprachnachrichten, Kalendereinträge für Besprechungen, Kontakte u. Ä.) sowie weitere zusätzliche Informationen, die die betroffene Person im Laufe des Kommunikationsaustauschs eventuell bereitstellt.

Wenn die betroffene Person eine externe Person ist:

- Kontaktinformationen: private und/oder berufliche E-Mail-Adresse
- Netzwerk-/Anwendungsinteraktionsdaten: Sitzungsmetadaten, Sitzungsinhalt, Sitzungsdetails

- Browsing-Informationen: IP-Adresse, Verlauf der aufgerufenen Websites, Datum und Uhrzeit von Browsing-Sitzungen, Netzwerkinteraktionsverlauf, Cookie-Informationen, URL, User-Agent des Browsers, Browser-Typ
- Sensorische und elektronische Informationen: Anwesenheitsstatus, Audioinformationen, visuelle Informationen
- Telefonie-Interaktionsdaten: Telefonie-Sitzungsmetadaten, Telefonie-Sitzungsinhalt, Telefonie-Sitzungsdetails
- Anrufinformationen: gewählte Rufnummer, Rufnummer des Anrufers, Datum und Uhrzeit von Anrufen, Anrufdauer, Anrufliste, Anruf-Interaktionsverlauf.
- Systemprotokolle: Webserver-Protokolle, system-/anwendungs-/sicherheitsbezogene Serverprotokolle
- Personenbezogene Informationen, die die betroffene Person im Rahmen der Dateifreigabe für berufliche Tätigkeiten freiwillig bereitstellt (z. B. Nachrichten, Bilder, Dateien, Sprachnachrichten, Kalendereinträge für Besprechungen, Kontakte u. Ä.) sowie zusätzliche Informationen, die die betroffene Person im Laufe des Kommunikationsaustauschs eventuell bereitstellt.

3. Wer ist für die Verarbeitung der Daten verantwortlich?

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

Die Verarbeitung personenbezogener Daten erfolgt durch Bedienstete der Hauptdirektion 4.6, die mit der Verwaltung der in dieser Erklärung genannten Anwendungen befasst sind.

Externe Anbieter, die mit dem Support, dem Betrieb und der Wartung für Microsoft-365-Anwendungen befasst sind – u. a. Microsoft selbst – können ebenfalls personenbezogene Daten verarbeiten und dabei ggf. auf diese Daten zugreifen.

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

Personenbezogene Daten werden bedarfsorientiert gegenüber folgenden Empfängern offengelegt:
• EPA-Bediensteten und externen Nutzern in für den Informationsaustausch genutzten Microsoft-365-Anwendungen (z. B. Teilnehmer eines MS-Teams-Meetings).
• Bediensteten der Hauptdirektion 4.6 des EPA, Microsoft-Mitarbeitern und Mitarbeitern externer Anbieter der Hauptdirektion 4.6, die mit der für die Bereitstellung der Dienstleistung erforderlichen Datenverarbeitung befasst sind.

In Microsoft 365 ist grundsätzlich der überwiegende Teil des Servicebetriebs automatisiert, um die Notwendigkeit eines menschlichen Zugriffs zu verringern. Jeder erforderliche Zugriff durch Microsoft ist zeitlich begrenzt und erfolgt mit eingeschränkten Zugriffsrechten.

Wird ein Online-Meeting in MS Teams aufgezeichnet, kann die Aufzeichnung unter Umständen – je nach Meeting – dem gesamten EPA oder über das EPA hinaus bereitgestellt werden. Die betroffene Person wird in jedem Fall vom Organisator des Meetings ordnungsgemäß über die Einzelheiten der Verarbeitung unterrichtet (z. B. mittels einer speziellen Datenschutzerklärung).

Bei mit MS Forms erstellten Umfragen/Formularen/Fragebögen werden die Fragen und Antworten in der Microsoft-Cloud gespeichert. Ausschließlich der Besitzer der Umfrage hat Zugriff auf die im Rahmen der jeweiligen Umfrage übermittelten Antworten. Im Falle einer anonymen Umfrage sind in der Antwort keine Kontaktinformationen der Teilnehmer ersichtlich. Bei vertraulichen Umfragen (= nicht anonym) hat der Besitzer Zugriff auf den Namen und die E-Mail-Adresse des Teilnehmers und auf Datum und Uhrzeit des Öffnens der Umfrage sowie der Übermittlung der Antwort durch den Teilnehmer.

5. Wie schützen wir Ihre personenbezogenen Daten?

Wir ergreifen angemessene technische und organisatorische Maßnahmen, um Ihre personenbezogenen Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust oder Veränderung 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 EPA 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.

Spezielle Maßnahmen in Verbindung mit der Aufzeichnung von MS-Teams-Meetings:

Bei der Aufzeichnung eines Online-Meetings können Teilnehmer die Verarbeitung ihrer personenbezogenen Daten durch die Aktivierung/Deaktivierung ihres Mikrofons und ihrer Kamera beschränken. Bei Vorliegen berechtigter Gründe können Teilnehmer darüber hinaus über die Chat-Funktion um eine vorübergehende Unterbrechung der Aufzeichnung bitten, damit ihr Beitrag nicht aufgezeichnet wird.

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 DSB 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."

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:

- Chats in Teams, Kanalnachrichten in Teams, Inhalte in OneDrive und SharePoint werden gespeichert, bis das EPA den Vertrag mit Microsoft kündigt.
- OneDrive: Personenbezogene Daten werden ein Jahr nach Löschung des Nutzerkontos automatisch von OneDrive gelöscht.
- MS Teams: Wird ein Chat oder eine Nachricht in Teams oder werden Inhalte in OneDrive und SharePoint Online von einem Nutzer gelöscht, werden sie nach der letzten Änderung ein Jahr lang in einem nur einem Administrator zugänglichen Bereich aufbewahrt, bevor sie endgültig gelöscht werden.

  Bei Teams wird die Anrufliste 90 Tage lang gespeichert und kann von Administratoren eingesehen werden; ein Endnutzer kann nur seine eigenen Anrufe der letzten 30 Tage sehen.

  Aufzeichnungen von Teams-Meetings, die unter Verwendung der Aufzeichnungsfunktion vorgenommen wurden, werden vor ihrer Löschung drei Monate lang aufbewahrt, es sei denn, die aufzeichnende Person legt etwas anderes fest.
  Aufzeichnungen von MS Teams Live Events werden 180 Tage lang gespeichert. Solche Aufzeichnungen können je nach Art des Meetings länger als ein Jahr gespeichert werden, wobei der Aufbewahrungszeitraum entsprechend dem Zweck der Aufzeichnung festgelegt wird.
  Ist eine Aufzeichnung vor dem Ende des Aufbewahrungszeitraums veraltet oder überholt, wird sie gelöscht.
  Die besondere Aufbewahrungsfrist wird in einer speziellen Datenschutzerklärung und/oder einem Haftungsausschluss mitgeteilt, die/der zusammen mit der Einladung zu dem Meeting versendet wird.
- MS Forms: Bei mit MS Forms durchgeführten Umfragen ist der Besitzer der Umfrage für die Festlegung, Mitteilung und manuelle Durchführung der beschlossenen Aufbewahrung verantwortlich.

Des Weiteren hat das EPA während der Laufzeit seines Vertrags mit Microsoft jederzeit die Möglichkeit, auf die in den Anwendungen gespeicherten Daten 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, 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.

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, 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.