

## **Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen der Verwaltung von Verteilerlisten für Sammel-E-Mails**

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.

Dieses Verzeichnis von Verarbeitungstätigkeiten bezieht sich auf die Verwaltung von Verteilerlisten für Sammel-E-Mails anhand des SendInBlue-Tools. Dieses Tool dient zur Versendung von Sammel-E-Mails, was neben der automatisierten Erfassung, Nutzung, Speicherung, Übermittlung und Löschung von E-Mail-Adressen und Standortinformationen, die für bestimmte Unterbereiche der Organisation oder externe Nutzer verwendet werden, auch das manuelle Hinzufügen neuer Datensätze und das manuelle Löschen von ausscheidenden Mitgliedern umfasst.

### **1. Wie erfolgt die Verarbeitung und wozu dient sie?**

Diese Datenschutzerklärung betrifft die Verarbeitung personenbezogener Daten im Rahmen der Verwaltung von Verteilerlisten für Sammel-E-Mails mit dem SendinBlue-Tool.

Konkret geht es beim wichtigsten Anwendungsfall um Sammel-E-Mails, die intern an EPA-Kolleginnen und -Kollegen adressiert sind, z. B. Sammel-E-Mails von der Amicale oder der Personalvertretung. Basierend auf genehmigten Business Cases (z. B. standortspezifische E-Mails) verwendet der versendende Bereich die zugehörige autorisierte E-Mail-Adresse (gemeinsame Mailboxen, die dem jeweiligen Bereich gehören), um Sammel-E-Mails an das Tool zu senden, das zuerst prüft, ob der Absender tatsächlich autorisiert ist, und dann die Mail an die entsprechende Verteilerliste weiterleitet. Die Verteilerlisten werden jeder autorisierten Versand-E-Mail-Adresse zugeordnet. Opt-out-Tracking erfolgt im Tool automatisch. BIT ist für die Implementierung, Einrichtung und Wartung der Umgebung für den Versand von Sammel-E-Mails verantwortlich. Die Verteilerlisten für die oben Genannten werden regelmäßig (in der Regel zweimal pro Monat) aus dem EPA-Telefonbuch extrahiert und von BIT in das Tool SendInBlue hochgeladen. Die Adressaten haben die Möglichkeit zu kündigen, indem sie sich von diesen Verteilerlisten abmelden.

Ein zweiter Anwendungsfall betrifft Sammel-E-Mails, die von bestimmten Geschäftsbereichen des Amts verschickt werden, auch an externe Empfänger (z. B. von der Patentakademie). In diesen Fällen müsste der Geschäftsbereich für BIT regelmäßig eine aktuelle Verteilerliste zum Hochladen in das Tool bereitstellen, da diese nicht aus dem Telefonbuch abgeleitet werden kann. Die spezifischen Geschäftsbereiche bleiben auch für die Opt-in-Bestätigung (Zustimmung) durch die Empfänger verantwortlich. Das Consent Management wird, falls erforderlich, von der jeweiligen Geschäftseinheit verwaltet.

In beiden Anwendungsfällen sind die Einheiten, die die E-Mails versenden, für den Inhalt ihrer Mitteilungen verantwortlich, auch für etwaige personenbezogene Daten, die darin enthalten sein können.

Deshalb werden, wie beschrieben, personenbezogene Daten für die Verwaltung von Sammel-E-Mail-Verteilerlisten verarbeitet.

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

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 oder Ausnahmen für bestimmte Fälle nach Artikel 10 DSV zur Anwendung kommen.

## **2. Welche personenbezogenen Daten verarbeiten wir?**

Die folgenden Kategorien personenbezogener Daten werden für **Bedienstete und Auftragnehmer** verarbeitet:

- Nutzerkontendaten: Nutzer-ID
- Browsing-Informationen: IP-Adresse
- persönliche Identifikation: vollständiger Name
- Korrespondenz: freiwillig zur Verfügung gestellte personenbezogene Daten
- Beschäftigungsangaben (Unternehmenseinheit, Dienort)
- Kontaktinformationen: E-Mail-Adresse (geschäftlich), Kontaktdetails, Land, Privatadresse, Telefonnummern

Die folgenden Kategorien personenbezogener Daten werden für **Externe** verarbeitet:

- Browsing-Informationen: IP-Adresse
- Kontaktinformationen: E-Mail-Adresse (geschäftlich), Telefonnummern
- persönliche Identifikation: vollständiger Name

## **3. Wer ist für die Verarbeitung der Daten verantwortlich?**

Personenbezogene Daten werden unter der Verantwortung der Hauptdirektion CIO des EPA verarbeitet, die als delegierter Datenverantwortlicher des EPA handelt.

Externe Auftragnehmer, die an der Bereitstellung der Dienste 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?**

Personenbezogene Daten werden bedarfsorientiert für die Zwecke der Verwaltung des Dienstes für EPA-Bedienstete in BIT offengelegt.

Personenbezogene Daten können für Dritte zum Zwecke der Bereitstellung des Dienstes, der Wartung und der Unterstützung offengelegt 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 angemessene technische und organisatorische Maßnahmen, um Ihre personenbezogenen Daten vor versehentlicher oder rechtswidriger Vernichtung, Verlust oder Veränderung sowie unbefugter Offenlegung oder unbefugtem Zugang zu schützen.

Alle personenbezogenen Daten werden in sicheren IT-Anwendungen gemäß den Sicherheitsstandards des EPA gespeichert. Angemessener Zugriff wird 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-Zugriffskontrollen, weitere Zugriffskontrollen für das Rechenzentrum, Richtlinien für das Verschließen 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

Das EPA verwendet grundsätzlich ein papierloses Verwaltungssystem. Wenn dennoch Papierakten mit personenbezogenen Daten in den EPA-Gebäuden gelagert werden müssen, werden sie an einem sicheren verschlossenen und zugangsbeschränkten Ort aufbewahrt.

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 auch die technischen und organisatorischen Maßnahmen im Rahmen der verbindlichen Vereinbarung bewertet und überprüft. In diesen Systemen müssen geeignete technische und organisatorische Maßnahmen umgesetzt worden sein, wie z. B. physische Sicherheitsmaßnahmen, Zugriffs- und Speicherkontrollmaßnahmen, Sicherung von ruhenden Daten (z. B. durch Verschlüsselung), Benutzer-, Übertragungs- und Eingabekontrollmaßnahmen (z. B. Netzwerk-Firewalls, Network Intrusion Detection System (IDS), Network Intrusion Protection System (IPS), Auditprotokollierung) und Transportkontrollmaßnahmen (z. B. Sicherung von Daten bei der Übertragung durch Verschlüsselung).

## **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).

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](mailto:DPOexternalusers@epo.org) oder andernfalls als interner Nutzer an den delegierten Datenverantwortlichen unter [DP\\_BIT@epo.org](mailto: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](#) und als interner Nutzer dieses [Formular](#) auszufüllen und zusammen 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: 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. Bei EPA-Bediensteten, jungen Fachkräften und Abgeordneten nationalen Sachverständigen werden die Daten mit dem Ausscheiden aus dem Amt gelöscht. Personenbezogene Daten von externen Personen, einschließlich Mitgliedern der Öffentlichkeit, die sich mit Opt-in für eine Liste entscheiden und nicht abmelden, werden gelöscht, sobald die Verteilerliste eingestellt wird. Personenbezogene Daten von externen Personen, die sich abgemeldet haben, werden gelöscht, wenn der entsprechende Geschäftsbereich in regelmäßigen Abständen eine aktualisierte Verteilerliste bereitstellt.

Am Ende des Vertragsverhältnisses verpflichtet sich SendinBlue, alle personenbezogenen Daten innerhalb von höchstens drei (3) Monaten zu vernichten, vorbehaltlich der Verpflichtung von SendinBlue, Daten für rechtliche Zwecke zu speichern.

### **9. Kontaktinformationen**

Bei Fragen zur Verarbeitung ihrer personenbezogenen Daten können sich externe betroffene Personen schriftlich an den delegierten Datenverantwortlichen wenden unter [dpoexternalusers@epo.org](mailto:dpoexternalusers@epo.org). EPA-Bedienstete wenden sich bitte an den delegierten Datenverantwortlichen unter [DP\\_BIT@epo.org](mailto:DP_BIT@epo.org). Interne Bedienstete erreichen die Datenschutzbeauftragte unter [dpo@epo.org](mailto: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.