Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen der operativen Nutzung von FIPS (SAP)/myFIPS in HD 4.1 und HD 4.7

Der Schutz Ihrer Privatsphäre ist für das Europäische Patentamt (EPA) von höchster Bedeutung. Bei der Erfüllung unserer Aufgaben und der Erbringung unserer Dienstleistungen sehen wir uns dem Schutz Ihrer personenbezogenen Daten und der Wahrung Ihrer Rechte als betroffene Person verpflichtet. Alle Daten persönlicher Art, anhand derer Sie direkt oder indirekt identifizierbar sind, werden rechtmäßig, fair und mit der gebotenen Sorgfalt verarbeitet.

Die im Folgenden beschriebenen Verarbeitungen erfolgen nach den Datenschutzvorschriften des EPA (DSV).

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

Im Einklang mit der Finanzordnung verarbeiten die HD 4.1 und die HD 4.7 in FIPS verfügbare Daten, um Beschaffungsprozesse und Zahlungen zu erleichtern.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

FIPS (SAP) und myFIPS (Online-Schnittstelle für FIPS) werden in den Bereichen Finanzen und Beschaffung verwendet, um alle für die Finanz- und Beschaffungsprozesse erforderlichen Betriebsdokumente zu protokollieren und zu speichern. SAP ist zwar ein integriertes System, das auch den HR-Teil umfasst, hier werden aber nur die Teile abgedeckt, die die Beschaffungsprozesse direkt betreffen.
FIPS wird ganzheitlich für die Buchung von Dokumenten verwendet und beinhaltet aus verschiedenen Anwendungen dort gespeicherte Dokumentationen, um für alle beteiligten Bediensteten volle Transparenz von Entscheidungen zu gewährleisten. Die wichtigsten abgedeckten Prozesse sind Planung, Haushaltsaufstellung, Mittelreservierung, Sourcing, Vertragsmanagement, Einkauf/Bestellung, Abnahme von Waren/Dienstleistungen, Rechnungsstellung, Zahlungen, Cash-Management, PSCD, Vertrieb und Einnahmen, Controlling, Stammdaten, Berichterstattung, Nutzerverwaltung usw. Die meisten der EPA-Bediensteten, die mit der Genehmigung verschiedener Phasen der Prozess-, Berichterstattungs-, Controlling- und operativen Tätigkeiten betraut sind, sind mit allen vorgenannten Prozessen befasst. Daher werden mehrere Informationsdatenquellen verarbeitet, die im Tool protokolliert werden, um die Überprüfbarkeit und eine korrekte Prozesskontrolle zu gewährleisten. Der Zugriff auf die Daten wird von der IT-Abteilung des EPA, die System- und Governance-Bestimmungen einhalten muss, zentral und bedarfsorientiert verwaltet. Bei den operativen Aufgaben sind die Bediensteten selbst dafür verantwortlich, alle Informationen und Dateien hinzuzufügen, die für die interne Genehmigung und Überprüfbarkeit von Beschaffungsbuchungen erforderlich sind.
Neben internen Bediensteten haben auf einige spezifische Informationen (basierend auf genehmigten Anfragen) auch Rechnungsprüfer, IT-Unterstützungspersonal (intern oder extern), an Projekten beteiligte Berater und Vertragsmanager Zugriff.

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?

Betroffene Personen sind EPA-Bedienstete und Angestellte externer Dienstleister. Verarbeitet werden können personenbezogene Daten folgender Kategorien:

- SAP-Logs
- Kontaktinformationen: Kontaktdaten, Land, Mobiltelefonnummer, Telefonnummern, geschäftliche E-Mail-Adresse
- Korrespondenz: alle Informationen, die im Rahmen des Austausches möglicherweise übermittelt werden, Chat-Inhalte, freiwillig bereitgestellte persönliche Informationen
- Ausbildung und Qualifikationen (wie Aus- und Fortbildungshistorie, Bildungsabschlüsse, Sprachen, Erfahrung im Projektmanagement)
- Beschäftigungsdaten: Geschäftsbereich, Unternehmenseinheit, Abteilungsname und/oder -nummer, Nummer und Ablaufdatum des EPA-Zugangsausweises, Stellenbezeichnung, Zimmernummer
- Finanzdaten
- Persönliche Identifikationsdaten
- Systemprotokoll: Dateidaten (Name, Größe und/oder Hash, Registerdaten, SAP-Log)
- Ticketinformationen
- Kontaktinformationen: Kontaktdaten, Telefonnummer, geschäftliche E-Mail-Adresse
- Physisch und/oder digital identifizierbare Werte wie das digitale Zertifikat

Darüber hinaus werden Angaben zu Auftragnehmern und Bietern, die an Beschaffungsverfahren teilgenommen haben, zusammen mit der Information, ob an sie Aufträge vergeben wurden, verarbeitet.

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten werden unter der Verantwortung des Hauptdirektors Beschaffung und Lieferantenmanagement, HD 4.7, verarbeitet, der als delegierter Datenverantwortlicher des EPA handelt.

Personenbezogene Daten werden von den Bediensteten des EPA verarbeitet, die an der Verwaltung der in dieser Erklärung genannten Initiativen, Projekte oder Tätigkeiten beteiligt sind.

4. Wer hat Zugriff auf Ihre personenbezogenen Daten und wem gegenüber werden sie offengelegt?

Personenbezogene Daten werden bedarfsorientiert allen Bediensteten/Beratern/Rechnungsprüfern auf Grundlage der ihnen von der BIT-Abteilung zugeordneten Rollen offengelegt. Andere Beteiligte haben über Berichte Zugriff auf aggregierte operative Daten.

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 und sichern wir Ihre personenbezogenen Daten?

Die HD 4.7 ergreift 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. Angemessene Zugriffsberechtigungen werden individuell nur den oben genannten Empfängern gewährt.

Alle in FIPS/myFIPS enthaltenen personenbezogenen Daten werden in sicheren IT-Anwendungen unter Einhaltung der BIT-Sicherheitsstandards für das EPA gespeichert. Zu diesen 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 für die Systeme und das Netzwerk, Grundsätze der Bedarfsorientiertheit und der minimalen Berechtigung): Trennung in Administrator- und Nutzerrollen, Nutzer haben eine minimale Berechtigung, allgemeine Administratorrollen werden auf ein Minimum beschränkt
- Verstärkung der logischen Sicherheit von Systemen, Ausrüstung und Netzwerk: 802.1X für den Netzwerkzugriff, Verschlüsselung von Endgeräten, Virenschutzsoftware auf allen Geräten
- Physischer Schutz: EPA-Zugangskontrollen, zusätzliche Zugangskontrollen für das Rechenzentrum, Regeln für das Abschließen von Büros
- Reaktion auf sicherheitsrelevante Vorfälle: Rund-um-die-Uhr-Überwachung auf Vorfälle, Sicherheitsexperte in Bereitschaft, Zertifizierung Dritter

Prinzipiell hat das EPA ein papierloses Verwaltungssystem eingeführt. Wenn dennoch Papierakten mit personenbezogenen Daten in den EPA-Gebäuden gelagert werden müssen, werden sie an einem sicheren abgesperrten und zugangsbeschränkten Ort aufbewahrt.
Wenn Daten outgesourct (z. B. extern gespeichert, zugänglich gemacht und verarbeitet) werden, wird eine Risikobewertung für Datenschutz und Sicherheit durchgeführt, und folgende allgemeine Erklärung könnte aufgenommen werden:

Für personenbezogene Daten, die mit nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, haben sich die die personenbezogenen Daten verarbeitenden Anbieter in einer rechtsverbindlichen Vereinbarung verpflichtet, die sich aus dem anwendbaren Datenschutzrahmen ergebenden Verpflichtungen zu erfüllen. Das EPA hat außerdem eine Überprüfung der Datenschutz- und Sicherheitsrisiken durchgeführt. In diesen Systemen müssen geeignete technische und organisatorische Maßnahmen umgesetzt worden sein, so z. B. physische Sicherheitsmaßnahmen, Zugriffs- und Speicherkontrollmaßnahmen, Sicherung von ruhenden Daten (z. B. durch Verschlüsselung), Nutzer-, Übertragungs- und Eingabekontrollmaßnahmen (z. B. Netzwerk-Firewalls, System zur Erkennung unberechtigter Netzwerkzugriffe (Intrusion Detection System, IDS), System zur Abwehr unberechtigter Netzwerkzugriffe (Intrusion Protection System, IPS), Auditprotokollierung), Transportkontrollmaßnahmen (z. B. Datensicherung bei der Übertragung durch Verschlüsselung).

6. Wie können Sie auf Ihre Daten zugreifen, sie berichtigen oder sie abrufen? Wie können Sie die Löschung Ihrer Daten verlangen oder ihre 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 PDCProcurement-dpl@epo.org an den delegierten Datenverantwortlichen. Damit wir schneller und genauer darauf antworten können, brauchen wir stets bestimmte Vorabinformationen. Wir empfehlen Ihnen daher, dieses Formular (für Interne) auszufüllen und es mit Ihrem Antrag einzureichen.

Wir bearbeiten Ihren Antrag so schnell wie möglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Gemäß Artikel 15 (2) DSV kann dieser Zeitraum jedoch um zwei Monate verlängert werden, wenn dies aufgrund der Komplexität und der Anzahl eingegangener Anträge erforderlich sein sollte. Über eine Verzögerung werden wir 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 Verwaltung und die Arbeitsweise des EPA erforderlich, wobei nicht alle für die Arbeitsweise des EPA erforderlichen Verarbeitungsvorgänge ausdrücklich durch das EPÜ vorgeschrieben sind.
Darüber hinaus werden personenbezogene Daten gemäß der Finanzordnung erhoben und verarbeitet (Weisung über die Ausführung des Haushaltsplans, Vergaberichtlinien, Weisung für Verträge, Richtlinie zur Ergänzung verschiedener Bestimmungen der Finanzordnung).

8. Wie lange speichern wir Ihre Daten?

Es gibt vordefinierte gesetzliche Anforderungen bezüglich Vertrags- und Rechnungsbuchungen, und eine Richtlinie zur Datenaufbewahrung ist in Arbeit.

9. Kontaktinformationen

Bei Fragen zur Verarbeitung Ihrer personenbezogenen Daten wenden Sie sich bitte schriftlich unter PDCProcurement-DPL@epo.org an den delegierten Datenverantwortlichen.

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.