Datenschutzerklärung zur Verarbeitung personenbezogener Daten durch den EPA-Dienst Microsoft Defender for Endpoint

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 betrifft die Verarbeitung sicherheitsrelevanter Daten durch den EPA-Dienst Microsoft Defender for Endpoint (MDE). Die Daten werden von integrierten Endpunkten (Windows-Workstations und Windows-Servern) gesammelt und an einen separaten Cloud-Tenant übertragen, der vom MDE-Dienst des EPA für die automatisierte Verarbeitung und Warnung genutzt wird. Die Hauptdirektion (HD) 4.6 des Bereichs Business Information Technology (BIT) sammelt Daten im Zusammenhang mit MDE-Sicherheitswarnungen des MDE-Cloud-Tenants und speichert sie automatisiert vor Ort in Splunk.

Das EPA verarbeitet personenbezogene Daten zu folgenden Zwecken:

- Verhinderung von Sicherheitsvorfällen, die das Netzwerk und die Daten des EPA betreffen (z. B. Malware-Infektionen)
- Aufspürung und Meldung schädlicher oder böswilliger Aktivitäten auf Endpunkten in der Infrastruktur des EPA
- Untersuchung und Behebung von Sicherheitsvorfällen in der Infrastruktur des EPA

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?

Folgende Kategorien personenbezogener Daten werden verarbeitet:

Die betroffene Person ist EPA-Bedienstete/r oder Auftragnehmer des EPA (bei einem externen Dienstleister angestellt):

- Persönliche Identifikation: Vorname, Nachname
- Kontaktdaten: Telefonnummern, geschäftliche E-Mail-Adresse
- Nutzerkonto: Kontonummer, Nutzer-ID
- Beschäftigungsangaben: Stellenbezeichnung/Rolle, Abteilungsbezeichnung und/oder -nummer

- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsinformationen, Sitzungsmetadaten
- Browsing-Informationen: Dauer, Datum und Uhrzeit, Browsertyp, IP-Adresse, Kategorie, URL, Websiteverlauf, Netzwerkinteraktionsverlauf
- Geräteverwaltungsdaten: Geräte-ID Azure Active Directory
- Physische und/oder digitale identifizierbare Ressourcen: MAC-Adresse des Workstation-Netzwerkadapters, Seriennummer der Workstation, Betriebssystemversion, (physischer oder virtueller) Hostname sowie Hersteller und Modell der Workstation, BIOS-Version, Prozessortyp, installierte Browser-Erweiterungen einschließlich ihres Status (aktiv/inaktiv), installierte Zertifikate mit Angaben zu ihren Eigenschaften, installierte Softwareanwendungen
- Systemprotokolle: Überwachungsprotokolle (Audit Trails), system-, anwendungs- und sicherheitsbezogene Serverprotokolle, Registry-Daten, laufende Prozesse, Portnummern, Dateidaten (Name, Größe und/oder Hash)

Die betroffene Person ist eine externe Person:
- Browsing-Informationen: Dauer, IP-Adresse, Netzwerk-/Anwendungs-Interaktionsdaten, Sitzungsmetadaten

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 von den Bediensteten der BIT-Abteilung 4.6.2.3 Informationssicherheit verarbeitet, die an der Verwaltung des in dieser Erklärung genannten Dienstes beteiligt sind.

Externe Auftragnehmer, die an der Unterstützung und Wartung der Microsoft-Anwendung beteiligt sind – einschließlich Microsoft selbst –, können ebenfalls auf die personenbezogenen Daten zugreifen und diese verarbeiten.

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

Personenbezogene Daten werden über die Bedienkonsole des MDE-Cloud-Tenant bedarfsorientiert für folgende Empfänger offengelegt:
- bestimmte EPA-Bedienstete der BIT-Abteilung 4.6.2.3-Informationssicherheit (ausschließlich namentlich benannte Personen)
- namentlich benannte Personen in der HD 4.6 mit der Rolle Microsoft O365 Global Administrator oder Microsoft O365 Reader

Personenbezogene Daten können für im Namen von BIT handelnde Dritte zum Zwecke der Datenpflege und der Unterstützung offengelegt werden. Grundsätzlich sind die meisten Servicevorgänge für Microsoft-Produkte automatisiert, um den Bedarf für menschlichen Zugriff zu reduzieren. Jeder erforderliche Zugriff ist zeitlich begrenzt und unterliegt beschränkten Zugriffsrechten.

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.

Für personenbezogene Daten, die mit nicht in den Räumlichkeiten des EPA gehosteten Systemen verarbeitet werden, hat das EPA eine Risikobewertung für Datenschutz und Sicherheit durchgeführt. Die die personenbezogenen Daten verarbeitenden Anbieter haben sich in einer rechtsverbindlichen Vereinbarung verpflichtet, die sich aus dem anwendbaren Rechtsrahmen für den Datenschutz ergebenden Verpflichtungen zu erfüllen.

Alle personenbezogenen Daten, die über öffentliche Netzwerke zwischen dem EPA und Microsoft oder zwischen Microsoft-Rechenzentren übertragen werden, werden standardmäßig verschlüsselt. Auch ruhende personenbezogene Daten, die Microsoft vom oder im Namen des EPA im Rahmen der Verwendung des Dienstes Microsoft Defender for Endpoint zur Verfügung gestellt werden, werden verschlüsselt. Microsoft verwendet dafür modernste Verschlüsselungstechnologien. Darüber hinaus nutzt Microsoft Zugriffsmechanismen, die auf dem Grundsatz der geringsten Berechtigung beruhen, um den Zugriff auf vom EPA zur Verfügung gestellte personenbezogene Daten zu kontrollieren. Eine rollenbasierte Zugriffssteuerung wird eingesetzt, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf personenbezogene Daten einem angemessenen Zweck dient und vom Management genehmigt ist. Jeder erforderliche Zugriff auf Microsoft-Dienste durch Microsoft ist zeitlich begrenzt.

Microsoft implementiert und verwaltet mehrere Sicherheitsmaßnahmen zum Schutz personenbezogener Daten, die Microsoft durch die Verwendung des Dienstes Microsoft Defender for Endpoint Microsoft durch das EPA zur Verfügung gestellt werden. Diese Sicherheitsmaßnahmen umfassen die Organisation der Informationssicherheit (z. B. Sicherheitsverantwortung, Sicherheitsrollen und -zuständigkeiten, Risikomanagement-Programm), die Bestandsverwaltung (z. B. Bestandsverzeichnis und -nutzung), Personalsicherheit (z. B. Sicherheitsschulungen), physische und ökologische Sicherheit (z. B. physischer Zugang zu Anlagen, physischer Zugang zu Komponenten, Schutz vor Störungen, Entsorgung von Komponenten), Kommunikations- und Betriebsmanagementkontrollen (z. B. Betriebsrichtlinien, Datenwiederherstellungsverfahren, Anti-Malware-Kontrollen, Ereignisprotokollierung), Zugriffskontrollmaßnahmen (z. B. Zugriffsrichtlinien, Zugriffsberechtigungen, Least-Privilege-Prinzip, Integrität und Vertraulichkeit, Authentifizierung, Netzwerkdesign), Management von Informationssicherheitsvorfällen (z. B. Prozesse für die Reaktion auf Vorfälle, Überwachung von Diensten) und die Verwaltung der Geschäftskontinuität. Microsoft implementiert und unterhält außerdem geeignete technische und organisatorische Maßnahmen zum Schutz anderer personenbezogener Daten, die sich von den oben beschriebenen unterscheiden. Diese Maßnahmen sind in der Microsoft-Sicherheitsrichtlinie beschrieben.

Microsoft Defender for Endpoint wurde so konfiguriert, dass durch die vorstehend genannten Maßnahmen die Vertraulichkeit der Informationen gewahrt wird. Der anonyme Zugriff ist nicht gestattet. Informationen, die über Microsoft Defender for Endpoint gesammelt werden, sind nur für die in Abschnitt 4 genannten spezifischen Nutzer und Gruppen zugänglich.

Microsoft Defender for Endpoint ist nach mehreren Sicherheitsstandards zertifiziert, darunter ISO27001, SOC1 Typ II, SOC2 Typ II und ISO27018 (Leitfaden zum Schutz personenbezogener Daten in Cloud-Diensten) und erfüllt die Anforderungen der Norm ISO27002.

Microsoft führt jährlich eine Sicherheitsprüfung der Computer, der Computerumgebung und der physischen Rechenzentren durch, die personenbezogene Daten verarbeiten. Die Prüfungen werden von unabhängigen, externen Prüfern entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder Rahmenbestimmungen durchgeführt.

Die personenbezogenen Daten werden in der EU gemäß der vom EPA implementierten Anwendungskonfiguration gespeichert. Sie können jedoch Unterauftragnehmern zur Verarbeitung in anderen Ländern abhängig von den Erfordernissen bezüglich Wartung, Unterstützung oder Betrieb von cloudbasierten Diensten und der Verfügbarkeit dieses Know-hows zur Verfügung gestellt werden. Wird Zugriff auf die Daten gewährt, so geschieht dies befristet und nur für die Daten, die für das spezifische Wartungs-, Unterstützungs- oder Betriebsverfahren erforderlich sind. Die folgenden Sicherheitsmaßnahmen sind im Einsatz:

- Bei allen Transfers zur Verarbeitung in Drittländern schreibt Microsoft den Unterauftragnehmern Standardvertragsklauseln der EU für den Datentransfer vor.
- Microsoft verlangt, dass sich die Unterauftragnehmer für die Verarbeitung dem Microsoft Supplier Security and Privacy Assurance Program anschließen. Dieses Programm soll die Praxis der Datenverarbeitung standardisieren und stärken und gewährleisten, dass die Geschäftsprozesse und -systeme der Lieferanten mit denen von Microsoft konform sind.

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/oder die Verarbeitung Ihrer Daten zu beschränken (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. 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 baldmöglichst und in jedem Fall innerhalb eines Monats nach Eingang des Antrags 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?

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."

Personenbezogene Daten werden auf folgender Rechtsgrundlage verarbeitet: Rundschreiben Nr. 382 vom 29. März 2017 – Richtlinien des EPA 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. Genauer gesagt werden personenbezogene Daten gemäß den folgenden Aufbewahrungsregeln gespeichert:

- Die Daten werden maximal drei Tage in einem temporären Cache-Bereich im Endpunkt selbst gespeichert.
- Die Daten werden 180 Tage in der MDE-Cloud-Umgebung aufbewahrt und anschließend aus dem MDE-Cloud-Tenant gelöscht.

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 der personenbezogenen Daten können EPA-Bedienstete schriftlich den delegierten Datenverantwortlichen unter DP_BIT@epo.org kontaktieren, externe betroffene Personen wenden sich bitte an DPOexternalusers@epo.org.

Interne Nutzer erreichen unsere Datenschutzbeauftragte unter dpo@epo.org, externe Nutzer verwenden zu diesem Zweck die Adresse DPOexternalusers@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.