

Der Angemessenheitsverweis des EPA – ein Überblick



Einführung

Gemäß Artikel 9 (2) der Datenschutzvorschriften des Europäischen Patentamts (EPA DSV) ist die Übermittlung personenbezogener Daten an ein Land oder eine internationale Organisation nur zulässig, wenn das Land des Empfängers, ein Gebiet oder ein oder mehrere festgelegte Sektoren in diesem Land oder innerhalb der internationalen Organisation ein angemessenes Schutzniveau gewährleisten.

Das Konzept eines "angemessenen Schutzniveaus" bezieht sich auf das Schutzniveau personenbezogener Daten in dem Drittland oder der internationalen Organisation. Die Analyse umfasst den Inhalt der anwendbaren Vorschriften¹ und die Mittel zur Gewährleistung ihrer wirksamen Anwendung.

Angemessenheitsbeschlüsse des Präsidenten des Europäischen Patentamts (EPA) dienen der offiziellen Bestätigung, dass das von einem Land eines Empfängers oder einer internationalen Organisation gebotene Schutzniveau für personenbezogene Daten im Wesentlichen als dem des EPA gleichwertig angesehen werden kann.²

Das vorliegende Dokument beschreibt die Grundelemente eines Datenschutzrahmens und die Verfahrens- und Durchsetzungsmechanismen, die analysiert werden müssen, um zu bestimmen, ob der vom Land des Empfängers³ oder von einer internationalen Organisation gebotene Schutz aus datenschutzrechtlicher Sicht als angemessen gelten kann.

Angemessenheitsverweis

Der in einem Land oder einer internationalen Organisation geltende Datenschutzrahmen muss die folgenden grundlegenden Datenschutzgrundsätze und Verfahrens- bzw. Durchsetzungsmechanismen beinhalten.

1. Grundsätze, Rechte und Garantien

- 1.1. **Datenschutzrechtliche Kernkonzepte und/oder -grundsätze:** Die wichtigsten datenschutzrechtlichen Konzepte und/oder Grundsätze müssen mit denen des Datenschutzrahmens des EPA zwar nicht zwingend übereinstimmen, sollten sich jedoch an ihnen orientieren.⁴

¹ Einschließlich der Analyse des Rechtsrahmens für den Zugang von Behörden zu personenbezogenen Daten.

² Das Konzept des "angemessenen Schutzniveaus" wurde mit der Richtlinie 95/46 ins EU-Recht eingeführt und vom EuGH weiterentwickelt, insbesondere hinsichtlich der Vorgabe, dass zwar das "Schutzniveau" im Drittland oder der internationalen Organisation dem in der EU garantierten "der Sache nach gleichwertig" sein muss, sich aber "die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden" (siehe Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner, 6. Oktober 2015, §§ 73, 74). Obgleich EU-Recht keine Anwendung auf das EPA findet, hat der Datenschutzrahmen des EPA die Konzepte des "angemessenen Schutzniveaus" und der "Gleichwertigkeit der Sache nach" übernommen.

³ Als "Land des Empfängers" gelten Drittländer nach Artikel 3 (1) u) EPA DSV und Länder von Empfängern, die nicht von Artikel 8 (1), (2) und (5) EPA DSV umfasst sind.

⁴ Beispielsweise umfassen die EPA DSV folgende Kernkonzepte: "personenbezogene Daten", "Verarbeitung personenbezogener Daten", "Datenverantwortlicher", "Auftragsverarbeiter", "Empfänger" und "besondere Kategorien personenbezogener Daten".

- 1.2. **Gründe für eine gesetzmäßige Verarbeitung nach Treu und Glauben zu rechtmäßigen Zwecken:** Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und unter ausreichend klarer Darlegung der Rechtsgrundlagen verarbeitet werden.
- 1.3. **Grundsatz der Zweckbindung:** Personenbezogene Daten müssen zu konkreten Zwecken verarbeitet werden und dürfen demnach nur insofern genutzt werden, als dies dem Zweck der Verarbeitung nicht widerspricht.
- 1.4. **Grundsätze der Datenrichtigkeit und -minimierung:** Personenbezogene Daten sollten sachlich richtig und, erforderlichenfalls, auf dem neuesten Stand sein. Die Daten müssen für die Zwecke der Verarbeitung angemessen und dafür erheblich sein und dürfen nicht darüber hinausgehen.
- 1.5. **Grundsatz der Speicherbegrenzung:** Grundsätzlich dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, erforderlich ist.
- 1.6. **Grundsätze der Integrität und Vertraulichkeit:** Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet. Dies umfasst angemessene technische oder organisatorische Maßnahmen sowie den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.
- 1.7. **Grundsatz der Transparenz:** Betroffene Personen sind in klarer, leicht zugänglicher, knapper, transparenter und verständlicher Form über die wichtigsten Elemente der Verarbeitung ihrer personenbezogenen Daten zu informieren.
- 1.8. **Recht auf Auskunft, Berichtigung, Löschung und Widerspruch**
 - Betroffene Personen müssen das Recht haben, zu erfahren, ob sie betreffend Daten verarbeitet werden. Sie müssen darüber hinaus Auskunft über ihre Daten, einschließlich einer Kopie aller sie betreffenden Daten, die verarbeitet werden, erhalten können.
 - Betroffene Personen müssen das Recht haben, ihre Daten nach Notwendigkeit aus konkreten Gründen, beispielsweise bei nachweislicher Unrichtigkeit oder Unvollständigkeit, berichtigen zu lassen. Betroffene Personen müssen ferner das Recht haben, ihre personenbezogenen Daten löschen zu lassen, beispielsweise wenn die Verarbeitung der Daten nicht mehr erforderlich oder gesetzmäßig ist.
 - Betroffene Personen müssen ferner das Recht haben, der Verarbeitung ihrer Daten gemäß den spezifischen Bedingungen des Rechtsrahmens des jeweiligen Landes oder der internationalen Organisation jederzeit aus Gründen, die sich aus ihrer besonderen Situation ergeben, zu widersprechen. So haben betroffene Personen etwa laut den EPA DSV das Recht, der Verarbeitung ihrer personenbezogenen Daten nach Artikel 5 a) zu widersprechen, wenn die "Verarbeitung ... 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 [ist]".

Darüber hinaus darf die Ausübung besagter Rechte für betroffene Personen nicht übermäßig aufwendig sein; gleichzeitig können die Rechte möglichen Einschränkungen unterliegen.

- 1.9. **Besondere Kategorien personenbezogener Daten:** Im Falle besonderer Verarbeitungsarten sind weitere Garantien vorzuhalten. Sind beispielsweise "besondere Kategorien personenbezogener Daten" betroffen, sollten strengere Anforderungen festgelegt werden, z. B. die ausdrückliche Einwilligung der betroffenen Person zu der Verarbeitung oder die Bereitstellung geeigneter Garantien zum Schutz der Rechte und Freiheiten der betroffenen Personen.
- 1.10. **Automatisierte Entscheidungsfindung und Profiling:** Entscheidungen ausschließlich auf Grundlage automatisierter Verarbeitung ("automatisierte Entscheidungsfindung im Einzelfall"), einschließlich Profiling, die Rechtsfolgen nach sich ziehen oder sich erheblich auf die betroffene Person auswirken, sind nur unter bestimmten, im Rechtsrahmen des Landes des Empfängers oder der internationalen Organisation festgelegten Bedingungen zulässig. Gemäß den EPA DSV umfassen derartige Bedingungen beispielsweise das Erfordernis der ausdrücklichen Einwilligung der betroffenen Person oder der Notwendigkeit einer solchen Entscheidung, um einen Vertrag zwischen der betroffenen Person und dem Datenverantwortlichen zu schließen oder zu erfüllen. Entspricht die Entscheidung nicht den besagten, im Rechtsrahmen des Landes oder der internationalen Organisation verankerten Bedingungen, muss die betroffene Person sich ihr entziehen können. Der Rechtsrahmen des Landes oder der internationalen Organisation muss in jedem Fall notwendige Garantien vorsehen, darunter das Recht auf Information über die konkreten, der Entscheidung zugrunde liegenden Gründe und die damit verbundene Logik, das Recht auf Berichtigung unrichtiger oder unvollständiger Informationen durch menschliches Eingreifen sowie das Recht betroffener Personen, ihren Standpunkt zum Ausdruck zu bringen und die Entscheidung anzufechten, wenn diese auf Grundlage eines unrichtigen Sachverhalts getroffen wurde.
- 1.11. **Vorschriften zu Weiterübermittlungen:** Das Schutzniveau für personenbezogene Daten betroffener Personen darf nicht durch Weiterübermittlungen untergraben werden. Weitere Übermittlungen personenbezogener Daten durch den ursprünglichen Empfänger sind nur zulässig, wenn der nachfolgende Empfänger (d. h. der Empfänger der Weiterübermittlung) ebenfalls Vorschriften (einschließlich vertraglicher Pflichten) unterliegt, die ein angemessenes Schutzniveau bieten, sofern die einschlägigen Weisungen im Falle der Datenverarbeitung im Auftrag des Verantwortlichen befolgt werden, die Verarbeitung nur zu beschränkten und festgelegten Zwecken erfolgt und es eine Rechtsgrundlage dafür gibt.

2. **Verfahrens- und Durchsetzungsmechanismen**

Oggleich sich die Rechtsschutz- und Aufsichtsmechanismen, die ein Land oder eine internationale Organisation betroffenen Personen bietet, von denen des EPA unterscheiden können, muss der

entsprechende Datenschutzrahmen folgende Elemente umfassen, um bewerten zu können, ob das Schutzniveau des Landes oder der internationalen Organisation angemessen ist.

- 2.1. Funktionierender Aufsichtsmechanismus: Ein oder mehrere unabhängige Aufsichtsmechanismen oder Aufsichtsbehörden, die mit der Überwachung, Gewährleistung und Durchsetzung der Einhaltung von Bestimmungen über den Schutz von Daten und der Privatsphäre in einem Land oder einer internationalen Organisation betraut sind. Der Aufsichtsmechanismus handelt bei der Erfüllung seiner Pflichten und der Ausübung seiner Befugnisse unabhängig und unparteiisch, wobei er Weisungen weder erbittet noch annimmt. In diesem Zusammenhang muss der Aufsichtsmechanismus über die nötigen Befugnisse und Mandate verfügen, um die Einhaltung der Datenschutzrechte zu gewährleisten und dafür zu sensibilisieren.
- 2.2. Sichere Einhaltung: Das Datenschutzsystem sollte sämtliche folgenden Aspekte gewährleisten:
 - (i) ein hohes Maß an Rechenschaftspflicht,
 - (ii) ein umfassendes Bewusstsein von Datenverantwortlichen und Personen, die personenbezogene Daten in ihrem Auftrag verarbeiten, für ihre Verpflichtungen, Aufgaben und Verantwortlichkeiten,
 - (iii) eine Sensibilisierung und Aufklärung betroffener Personen für ihre Rechte und die Mittel zu ihrer Ausübung.
- 2.3. Rechenschaftspflicht: Der Datenschutzrahmen eines Landes oder einer internationalen Organisation muss Datenverantwortliche und Personen, die personenbezogene Daten in ihrem Auftrag verarbeiten, binden und verpflichten, seine Einhaltung – insbesondere gegenüber der zuständigen Aufsichtsbehörde – nachweisen zu können.⁵
- 2.4. Unterstützung und Hilfe für betroffene Einzelpersonen bei der Ausübung ihrer Rechte und Anwendung geeigneter Rechtsschutzmechanismen: Einzelpersonen müssen mittels Rechtsbehelfen ihre Rechte schnell, wirksam und zu erschwinglichen Kosten durchsetzen können, was ebenfalls die Einhaltung des Datenschutzes gewährleisten soll. Hierzu bedarf es Aufsichtsmechanismen, über die in der Praxis Beschwerden unabhängig geprüft und etwaige Verletzungen der Rechte auf Datenschutz und Privatsphäre identifiziert und geahndet werden können. Werden Vorschriften nicht eingehalten, müssen betroffene Personen auf wirksame behördliche und gerichtliche Rechtsbehelfe zugreifen können, um etwa Schadenersatz für die unrechtmäßige Verarbeitung ihrer personenbezogenen Daten zu erhalten. Dieser Kernaspekt muss ein System für unabhängige Entscheidungen oder Schlichtungen umfassen, worüber die Zahlung von Schadenersatz und ggf. die Verhängung von Rechtsfolgen möglich ist.

⁵ Beispielsweise durch die Verpflichtung zur Datenschutzerklärung.