DAS ENDE VON PRIVACY SHIELD

WAS SIND DIE HANDLUNGSOPTIONEN?

Nach dem Ende von Privacy Shield stellen sich viele Unternehmen die gleiche Frage: Was sind nun die verschiedenen Handlungs-Optionen – und welche Vor- und Nachteile haben sie?

Denn es gibt durchaus mehrere Möglichkeiten, die nach dem EuGH Urteil zur Verfügung stehen. Wir präsentieren und bewerten sie – damit Sie eine qualifizierte Entscheidung über die weiteren Schritte treffen können.

Hinweis: Wir haben versucht, die Optionen **nach dem Risiko absteigend** zu beschreiben – die ersten Optionen sind also für die meisten Unternehmen voraussichtlich mit mehr Risiko behaftet als die nachfolgenden.

a) Abwarten und Tee trinken

Auch wenn es nicht unbedingt empfehlenswert ist, natürlich steht Ihnen auch diese Option offen: Einfach nicht auf das Urteil reagieren und erst einmal die weitere Entwicklung abwarten.

Dafür kann es sogar durchaus nachvollziehbare Argumente geben: Vielleicht ändern die USA ihre Überwachungsgesetze, möglicherweise gibt es bald eine politische Lösung (also ein neues Abkommen), eventuell bleiben die Datenschutzbehörden großteils untätig, vielleicht betrifft das vorerst nur andere (größere) Unternehmen.

Diese Option hat einen großen Vorteil: Sie verursacht keinen Aufwand. Doch der Nachteil ergibt sich durch das Risiko, das ein Unternehmen mit dieser (Nicht-) Entscheidung eingeht: Denn im Fall des Falles kann man einer Datenschutzbehörde nicht nachweisen, dass man angemessene Anstrengungen zum Umsetzen des EuGH-Urteils unternommen hätte.

Vermutlich kann man diese Option gut mit dem Fahren auf einer österreichischen Autobahn mit einer Geschwindigkeit von 150 km/h vergleichen: Das kann viele Jahre gut gehen – doch man kann auch schon morgen in eine Radarfalle tappen und muss dann die entsprechenden Konsequenzen tragen. Da hilft auch weder das Argument, dass viele andere ebenfalls so schnell unterwegs sind noch dass man das „schon immer so" gemacht hat; Strafe zahlen wird man wohl in jedem Fall müssen.

b) Mit „zwingend notwendig" argumentieren

Der Artikel 49 der DSGVO sieht eine Ausnahme vom Verbot der Datenübermittlung in nicht-sichere Drittländer unter bestimmten Voraussetzungen vor, wenn dies „zwingend notwendig" ist. Dem steht allerdings die Aussage des europäischen Datenschutzausschusses gegenüber, dass diese Ausnahme **nur für gelegentliche** Datenübermittlungen in Anspruch genommen werden kann.

Als Beispiel wird hier oft das Senden eines E-Mails an ein amerikanischen Reiseveranstalter genannt, um die eigene Buchung und die eines Mitreisenden zu bestätigen – das wäre durch d en Artikel 49 also gedeckt.

Die Frage des Risikos wird voraussichtlich hauptsächlich von zwei Punkten abhängen:

- Wie oft kommt die Datenübermittlung vor?
- Gibt es sinnvolle Alternativen?

Gerade der zweite Punkt kann bei der Argumentation sehr hilfreich sein: Wenn man beispielsweise eine amerikanische Software für die Steuerung von Maschinen einsetzt, für die es keine Alternative gibt und deren Verzicht bedeuten würde, dass das Unternehmen nicht fortgeführt werden kann, dann wird man wesentlich besser mit „zwingend notwendig" argumentieren können als für den Versand eines Newsletters (für den es in Europa Dutzende vergleichbare Alternativen gibt).

In Summe wird diese Option für viele Datenanwendungen **keine** ausreichende Grundlage (für den weiteren Einsatz amerikanischer Dienstleister sein); doch im Vergleich zu Option „nichts tun" kann man immerhin argumentieren, dass man sich dazu etwas überlegt hat.

c) Standard-Vertrags-Klauseln (SCC)

Die Standard Contractual Clauses (SCC) sind von der Europäischen Kommission vorgegebene Rahmenverträge, die ein Unternehmen mit seinem amerikanischen Dienstleister abschließen kann. Darin sichert der Dienstleister die Einhaltung des europäischen Datenschutzniveaus zu.

Das klingt nach einer einfachen Lösung, doch in der Praxis gibt es hier mehrere Stolpersteine:

a) Der Anbieter muss erst einmal bereit sein, diese SCC auch tatsächlich abzuschließen, wobei die SCC inhaltlich nicht verändert werden dürfen.
b) Sie als Auftraggeber (!) müssen sicherstellen, dass der Anbieter die Vorgaben überhaupt einhalten kann. Angesichts der Überwachungsgesetze in den USA ist jedoch derzeit davon auszugehen, dass ein amerikanischer Dienstleister diese Vorgaben gar nicht erfüllen kann.
c) Sie müssen auch die laufende Einhaltung des Datenschutz-Niveaus sicherstellen, da Sie letztendlich datenschutzrechtlich der Verantwortliche sind. Das wird in der Praxis nur schwer machbar sein.

Der Nachteil dieser Option ist also, dass die SCC in der Praxis in vielen Fällen keine brauchbare Grundlage für die Datenübermittlung in die USA bilden. Und der EuGH hat betont, dass die Datenschutzbehörden die Pflicht haben, einzugreifen, um Datenübermittlungen auszusetzen oder zu verbieten (Randnummer 134 des Urteils C-311/18, „Schrems II"), sollte ein gültiges Rechtsinstrument für eine Übermittlung fehlen und der Verantwortliche nicht tätig werden.

Der Vorteil ist jedoch, dass Sie so zumindest einen Teil des Risikos auf Ihren Anbieter überwälzen können. Ob Sie jedoch im Fall einer Strafe dieses Geld von Ihrem Anbieter tatsächlich bekommen werden, steht wohl auf einem anderen Blatt.

Tipp: Glauben Sie nicht den Beteuerungen vieler amerikanischer Dienstleister, dass durch die SCC eine ausreichende Grundlage für die Datenübermittlung vorliegen würde – dann das ist eben höchst

zweifelhaft. Dazu ein Zitat von Max Schrems (noyb) am Beispiel von Facebook: „Facebook nutzt weiter die SCCs obwohl der EuGH festgehalten hat, dass diese gegen US-Überwachungsgesetze keinen ausreichenden Schutz bringen und daher nicht genutzt werden dürfen."

d) Binding Corporate Rules (BCR) einsetzen

Die BCR sind ähnlich den Standardvertragsklauseln, nur dass hierbei ein Unternehmen sich selbst verbindliche Datenschutzregeln auferlegt (z.B. für den konzerninternen Datentransfer von multinationalen Unternehmen). Sie werden in der Praxis nur selten eingesetzt, da sich die SCC als das einfachere Instrument etabliert haben.

Außerdem wäre eine externe Zertifizierung oder eigene Prüfung erforderlich, um auf der Grundlage der BCR Daten in ein unsicheres Drittland zu transferieren, was aufgrund des Aufwands kaum durchführbar ist.

Zudem gelten die Vorbehalte gegenüber den SCC analog auch für die Binding Corporate Rules.

e) Keine personenbezogenen Daten speichern

Die DSGVO betrifft „nur" personenbezogene Daten. Damit betrifft auch das Ende von Privacy Shield nur solche Daten.

Daher wäre eine einfache Lösung, einfach keine personenbezogenen Daten zu übermitteln. Bei einem Newsletter-Anbieter wird das natürlich nicht möglich sein, doch bei manchen Anwendungen (z.B. einem Projektplan) kann man eventuell durchaus auf die Angabe von Namen verzichten.

Eine weitere Möglichkeit wäre, die personenbezogenen Daten zu verschlüsseln. Ein Beispiel dafür ist Boxcryptor: Mit diesem Tool können Sie Daten, die Sie in einer (amerikanischen) Cloud speichern, vorher verschlüsseln, so dass amerikanische Behörden keinen Zugriff auf die unverschlüsselten Daten haben.

f) Auf eine Lösung Ihres Anbieters warten

Es gibt natürlich auch für Ihren Anbieter die Möglichkeit, für die Datenübermittlungen für seine Kunden in Europa eine legale Grundlage zu schaffen. So könnte der Anbieter beispielsweise ein rechtlich eigenständiges Unternehmen in Europa gründen, das dann alle EU-Kunden betreut und deren Daten speichert, ohne dass die amerikanische „Mutter" Zugriff auf die Daten bekommt.

Ein Beispiel dafür war Microsoft, das den europäischen Kunden die Möglichkeit bot, die Daten auf Servern in der EU zu speichern, die jedoch nicht von Microsoft, sondern treuhänderisch von der deutschen Telekom verwaltet wurden. Selbst Microsoft hatte damit keinen Zugriff auf diese Daten – und die deutsche Telekom wiederum unterliegt nicht den amerikanischen Gesetzen. (Diese Lösung ist u.a. daran gescheitert, dass Microsoft dafür rund 20% höhere Preise für die europäischen Kunden verlangt hatte).

Ob weitere amerikanische Unternehmen solche oder ähnliche Lösungen schaffen werden, bleibt abzuwarten. Derzeit scheinen solche Lösungen allerdings leider nicht realistisch.

Hinweis: Es reicht nicht aus, wenn nur die Server in Europa stehen. Denn amerikanische Behörden können ja dennoch Zugriff auf die Daten erlangen. Wo die Server physisch stehen, spielt dabei weder technisch noch faktisch keine Rolle.

g) Zustimmung der Betroffenen einholen

Sie dürfen personenbezogene Daten auch weiterhin an den amerikanischen Dienstleister übermitteln, wenn die Betroffenen darüber informiert wurden und dem zugestimmt haben.

Es müssen allerdings sämtliche Betroffene eine freiwillige, spezifische, informierte und eindeutige Einwilligung abgegeben haben. Sie müssen also nachweislich über alle möglichen Risiken aufgeklärt worden sein.

Diese Einwilligung wird deshalb in der Praxis vermutlich nicht ganz einfach einzuholen sein. Außerdem gibt es einen Haken: Die Einwilligung kann durch den Betroffenen jederzeit – ohne Angabe von Gründen – widerrufen werden. Nach einem Widerruf wäre die Übermittlung der Daten also nicht mehr zulässig.

Und eine wichtige Frage bleibt noch offen: Was passiert mit den bestehenden Empfängern, die nicht über die Risiken aufgeklärt wurden und der Übermittlung zugestimmt haben? Von diesen nachträglich diese Zustimmung einzuholen, wird in der Praxis wohl kaum möglich sein.

h) Eine europäische Alternative suchen

Dieser Weg löst alle Ihre Probleme mit dem Ende von Privacy Shield. Denn wenn Sie für Ihre Datenanwendung einen europäischen Dienstleister einsetzen, bleiben die Daten im geschützten Raum der EU (solange der Anbieter keine amerikanischen Sub-Dienstleister einsetzt – das müssten Sie sicherstellen).

Bei vielen Anwendungen ist das gar nicht mal so viel Aufwand. So gibt es beispielsweise als Alternative zu Cloud-Speicherdiensten wie Dropbox oder Onedrive auch gleichwertige europäische Anbieter – und sogar kostenlose Open-Source Lösungen wir nextcloud oder owncloud.

Auch für E-Mail Marketing gibt es in Europa Dutzende gute Alternativen – auch hier muss man also nicht zwingend auf einen amerikanischen Anbieter zurückgreifen. (Wir können Sie bei der Auswahl gerne beraten).

Allerdings gibt es sicherlich auch Fälle für amerikanische Tools, für die es keine gleichwertige Alternativen in Europa gibt. Da bleibt nur die Option, eine längere Recherche in Kauf zu nehmen, auf die Anwendung zu verzichten oder Artikel 49 („zwingend notwendig", siehe oben) als Grundlage zu argumentieren oder auf eine baldige politische Lösung zu hoffen.

Übersicht: Alle Optionen im Vergleich

Welche der Maßnahmen sind nun besser oder weniger gut geeignet? Wir haben für die bessere Übersicht alle Maßnahmen nach drei Kriterien bewertet:

- Schutzpotential: Wie sehr könnte die Maßnahme das Problem lösen?

- Aufwand: Wie hoch wird der Aufwand für die Umsetzung vermutlich sein?
- Umsetzbarkeit: Wie wahrscheinlich ist es, dass die Maßnahme auch realisiert werden kann?

	Schutz	Aufwand	Umsetzbarkeit
Abwarten und Tee trinken	☹	🙂	🙂
Argumentation „zwingend notwendig"	☹	🙂	🙂
Standardvertragsklauseln	😐	😐	😐
Binding Corporate Rules	☹	😐	🙂
Keine personenbezogenen Daten	🙂	😐	🙂
Anbieter-Lösung abwarten	🙂	🙂	☹
Zustimmung der Betroffenen einholen	🙂	😐	😐
Alternativen recherchieren	🙂	☹	🙂

Empfehlung: Ausführliche Dokumentation

Egal, für welche Option – oder Kombination von Optionen – Sie sich entscheiden: Sie sollten unbedingt alle Schritte und Überlegungen ausführlich dokumentieren!

Denn im Fall einer Behördenanfrage oder einer Beschwerde durch einen Betroffenen können Sie so zumindest argumentieren, dass Sie das Thema ernst genommen und sich ausführlich damit auseinandergesetzt haben. So können Sie Ihr Risiko voraussichtlich deutlich reduzieren als wenn für Sie nach dem Urteil des EuGH einfach „business as usual" gilt.

Fazit: Datenschutz ist wichtiger als wirtschaftliche Interessen

Mit seinem Urteil hat der EuGH klar gemacht, dass die Menschenrechte (und damit nicht zuletzt der Datenschutz) vor wirtschaftliche Interessen zu stellen sind.

Nur weil ein amerikanischer Anbieter ein paar Euro günstiger ist als eine europäische Alternative, dürfen personenbezogene Daten der Betroffenen nicht einfach in ein nicht-sicheres Drittland übermittelt werden.

Damit stellt sich die Frage: Sollte dieses Prinzip nicht auch für Unternehmen gelten? Sollten nicht auch Unternehmen sorgsamer mit den ihnen anvertrauten Daten umgehen? Sollte das nicht mehr als eine wirtschaftliche Entscheidung sein?

Darüber hinaus kann man die DSGVO und den Datenschutz in Europa nicht nur als lästige Pflicht, sondern auch als **Chance** begreifen! Denn es gibt immer mehr Personen, die auf den Schutz ihrer Daten Wert legen – und bereit sind, das bei der Auswahl ihrer Dienstleister auch zu berücksichtigen.

ÜBER DIE E-MAIL MARKETING ACADEMY

Wir haben eine unendliche Leidenschaft für E-Mail Marketing. Denn kein Kanal erlaubt es, so zielgerichtet und individuell seine Zielgruppe zu erreichen und anderer Kanal macht es möglich, so einfach und effektiv einen echten Dialog zu etablieren.

So bieten wir Inhouse-Seminare und kompetente Beratung für alle Themen rund um E-Mail Marketing an. Vom halbtägigen Workshop bis zu mehrtägigen Intensiv-Seminaren, vom Newsletter-Gutachten bis zu individuellem Consulting.

Egal, ob Sie mit E-Mail Marketing beginnen, Ihren Newsletter nachhaltig verbessern oder als Profi noch etwas dazulernen möchten: Bei uns finden Sie kompetente Unterstützung von echten E-Mail Marketing Spezialisten.

E-Mail Marketing Academy | Mag. Michael Kornfeld
Nussgasse 31, 3434 Wilfersdorf
+43 2273 72788 | servus@email-marketing-academy.at
www.email-marketing-academy.at