FAQ ZU PRIVACY SHIELD

WELCHE KONSEQUENZEN HAT DAS EUGH URTEIL?

Das EuGH-Urteil, das zum Ende des Privacy Shield Abkommens zwischen der EU und den USA geführt hat, wirft für viele Unternehmen eine ganze Reihe von Fragen auf und sorgt für viel Unsicherheit: Darf ich amerikanische Dienstleister ab sofort nicht mehr einsetzen? Gibt es Ausnahmen? Wie hoch ist das Risiko? Mit welchen Strafen ist zu rechnen? usw.

In diesem Dokument wollen wir uns mit den häufigen Fragen zu dem Thema beschäftigen und möglichst verständliche und klare Antworten dazu liefern.

Wir behandeln folgende Fragen:

- Warum hat der EuGH das Abkommen eigentlich gekippt?
- Wieso ist bei den USA von "Überwachungsgesetzen" die Rede?
- Was sind die direkten Konsequenzen der EuGH Entscheidung?
- Wie lange ist die Übergangsfrist? Wie schnell muss ich reagieren?
- Ist eine baldige politische Lösung zu erwarten?
- Ist nun der Einsatz von allen amerikanischen Anbietern illegal?
- Ist eine Zustimmung durch die Betroffenen ausreichend?
- Sind notwendige Datenübermittlungen zulässig?
- Darf ich also zum Beispiel ab sofort kein E-Mail in die USA schicken?
- Können Verbraucher weiterhin Dienstleistungen in den USA in Anspruch nehmen?
- Was sind SCC (Standard Contractual Clauses)?
- Sind SCC eine ausreichende Basis für eine Datenübermittlung?
- Ist nicht der Anbieter für die Einhaltung der SCC verantwortlich?
- Betrifft das EuGH Urteil nur den Datentransfer in die USA?
- Ist mein Newsletter davon betroffen?
- Aber Mailchimp hat doch geschrieben…
- Und wenn die Server in Europa stehen?
- Sind Partner-Agenturen von Mailchimp & Co. betroffen?
- Muss ich gleich mit hohen Strafen rechnen?
- Wie hoch ist das Risiko und welche Konsequenzen drohen?

Diese FAQ sollen Ihnen dabei helfen, eine fundierte Entscheidung darüber zu treffen, ob Sie von dem Urteil des EuGH betroffen sind und welche Maßnahmen Sie eventuell treffen sollten.

Für weitere Fragen stehen wir Ihnen natürlich gerne zur Verfügung! Unsere Kontaktdaten finden Sie in der Fußzeile und am Ende dieses Dokuments.

Warum hat der EuGH das Abkommen eigentlich gekippt?

In aller Kürze: Was den Datenschutz betrifft, gelten die USA als "nicht-sicheres" Drittland, da dort kein ausreichender Schutz für personenbezogene Daten europäischer Personen gewährleistet ist. Deshalb hat die EU Abkommen mit den USA geschlossen, mit der sich teilnehmende amerikanische Anbieter verpflichtet haben, sich an europäische Datenschutz-Standards zu halten. So war die Datenübermittlung legal und damit der Einsatz amerikanischer Dienstleister möglich.

Doch die Sache hatte einen Haken: Die Abkommen waren schlecht gemacht und "das Papier nicht wert, auf dem sie geschrieben waren" (nach Ansicht des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein). Die Folge war, dass der EuGH im Jahr 2015 das Abkommen "Safe Harbor" und nun im Juli 2020 auch das Nachfolge-Abkommen "Privacy Shield" für unzulässig erklärt hat.

Wieso ist bei den USA von "Überwachungsgesetzen" die Rede?

Spätestens seit den Enthüllungen durch Edward Snowden, Glenn Greenwald & Co. ist klar, dass es sowohl kulturell als auch rechtlich große Unterschiede im Bereich Datenschutz zwischen den USA und der EU gibt. Das zeigt sich auch darin, dass es in den USA mehrere Gesetze gibt, die mit den europäischen Datenschutz-Grundsätzen schlicht unvereinbar sind.

Ein Beispiel dafür ist der amerikanische CLOUD Act: Damit können amerikanische Behörden Zugriffe auf die Infrastruktur amerikanischer Unternehmen erlangen, unabhängig von deren Standort. Das betrifft auch Daten europäischer Empfänger. Dabei können US-Behörden Unternehmen explizit untersagen, die Betroffenen darüber zu informieren, dass US-Behörden auf personenbezogene Daten zugegriffen haben. (Details finden Sie in unserem Artikel "Der US CLOUD Act: Pest oder Cholera?").

Ein weiteres Beispiel: FISA 702 ("Foreign Intelligence Surveillance Act") sieht vor, dass amerikanische Bürger vor einer ansatzlosen Datenüberwachung geschützt sind (das regelt der vierte Verfassungszusatz der USA), jedoch gilt das explizit nicht für die Bürger aller anderen Staaten. Diese Ungleichbehandlung ist unvereinbar mit den Grundsätzen der DSGVO.

Was sind die direkten Konsequenzen der EuGH Entscheidung?

Mit der Entscheidung sind Datentransfers zwischen europäischen Unternehmen und amerikanischen Anbietern, die sich ausschließlich auf das gekippte Abkommen (Privacy Shield) stützen, ab sofort nicht mehr möglich bzw. nicht legal.

Wie lange ist die Übergangsfrist? Wie schnell muss ich reagieren?

Es gibt **keine** Übergangsfrist. Wie schon bei dem Vorgänger-Abkommen "Safe Harbor" hat der EuGH das Abkommen schlicht für ungültig erklärt. Damit gilt automatisch und ab sofort der Zustand vor bzw. ohne Abkommen.

Ist eine baldige politische Lösung zu erwarten?

Nein. Durch das Urteil heißt es "zurück an den Start" für die Europäische Kommission. Aufgrund der Tatsache, dass der EuGH nun beide Abkommen für unzulässig erklärt hat (und dafür durchaus klare

Worte fand), kann die Kommission nicht einfach wieder auf die Schnelle ein drittes Abkommen verhandeln – das wäre politisch nicht durchsetzbar.

Es muss nun also auf politischer Ebene über einen Ausgleich der Interessen verhandelt werden. Das ist angesichts der großen Meinungsunterschiede zu dem Thema, der Unberechenbarkeit und des Egoismus der Trump-Regierung und aufgrund der bevorstehenden Wahlen in den USA sicher kein einfaches Unterfangen. Daher ist nicht in Wochen oder Monaten, sondern voraussichtlich erst in Jahren mit einer tragfähigen politischen Lösung zu rechnen.

Ist nun der Einsatz von allen amerikanischen Anbietern illegal?

Nein. Datenverarbeitungen für ausschließlich private Zwecke sind beispielsweise von der DSGVO überhaupt ausgenommen. Private Urlaubsfotos kann man also ohne rechtliche Bedenken in eine amerikanische Cloud hochladen.

Auch wenn gar keine personenbezogenen Daten gespeichert werden, ist die Datenübermittlung unbedenklich. Die Speicherung von Landschafts-Bildern oder einer Kostenaufstellung bei einem amerikanischen Anbieter ist also ebenfalls unproblematisch.

Außerdem dürfen unbedingt "notwendige" Datenübermittlungen weiterhin stattfinden. Sehen Sie dazu die Erklärungen weiter unten.

Darüber hinaus gibt es weitere Möglichkeiten, um auch personenbezogene Daten übermitteln zu dürfen. Eine davon ist die **informierte Zustimmung** durch den Betroffenen: Wenn der Betroffene also in die Übermittlung eingewilligt hat, ist sie auch legal möglich (siehe dazu nachfolgend).

Ist eine Zustimmung durch die Betroffenen ausreichend?

Grundsätzlich ja. Es müssen allerdings alle Betroffenen eine freiwillige, spezifische, informierte und eindeutige Einwilligung abgegeben haben. Sie müssen also nachweislich über **alle möglichen Risiken (!) aufgeklärt** worden sein.

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

Sind notwendige Datenübermittlungen zulässig?

Ja. Datenübermittlungen in die USA, die zwingend erfolgen müssen, sind auch weiterhin möglich und legal. Denn der Artikel 49 der DSGVO sieht hier eine Ausnahme vor. Das wurde vom EuGH auch bestätigt.

Als Beispiel wird hier oftmals ein E-Mail genannt, das man an ein amerikanisches Unternehmen schickt, um zum Beispiel eine Urlaubs-Buchung zu bestätigen – das ist also weiterhin erlaubt.

Der Knackpunkt ist jedoch, dass der Artikel 49 nur für gelegentliche Datenübermittlungen in Anspruch genommen werden kann. Deshalb kommt diese Ausnahme nach Artikel 49 nach Ansicht des Europäischen Datenschutzausschusses **nicht für laufende Datenübermittlungen** in Frage.

Ob außerdem der Einsatz eines amerikanischen E-Mail Marketing Dienstleisters zwingend "notwendig" ist, darf angesichts der Vielzahl von (guten) europäischen Alternativen bezweifelt werden.

Darf ich also zum Beispiel ab sofort kein E-Mail in die USA schicken?

Doch. In allen Fällen, wo das zwingend notwendig ist (zum Beispiel zur Vertragserfüllung), ist das weiterhin möglich.

Können Verbraucher weiterhin Dienstleistungen in den USA in Anspruch nehmen?

Ja. Denn jede Person darf wissentlich ihre eigenen (!) personenbezogenen Daten direkt in ein Drittland senden, zum Beispiel bei der Nutzung einer amerikanischen Website.

Es ist jedoch nicht möglich, Daten anderer Personen direkt mit einem US-Anbieter zu teilen, es sei denn, es wurde hierfür deren ausdrückliche Einwilligung eingeholt.

Was sind SCC (Standard Contractual Clauses)?

Es gibt die Möglichkeit, die Datenübermittlung durch die Verwendung von sog. SCC (Standard Contractual Clauses = Standard-Vertrags-Klauseln) zu legitimieren. Das sind standardisierte Verträge, die von der Europäischen Kommission erlassen wurden. Dadurch konnten europäische und amerikanische Unternehmen vertraglich regeln, dass bestimmte Datenschutz-Regeln gelten.

Sind SCC eine ausreichende Basis für eine Datenübermittlung?

Es ist sehr fraglich, ob aber die Standard-Vertragsklausel ausreichenden Schutz gegen die US-Gesetze bieten, weil sich die amerikanischen Unternehmen hier in einer Zwickmühle befinden: Entweder sie befolgen die nationalen Überwachungs-Gesetze (Verstoß wäre strafbar) oder die SCC bzw. die EU-Datenschutz-Gesetze (Verstoß wäre strafbar).

Die SCC bieten nur dann einen Schutz, wenn mehrere Bedingungen erfüllt sind:

- Die SCC der EU-Kommission müssen inhaltlich unverändert zwischen dem Unternehmen und dem Anbieter geschlossen werden.
- Ein solcher Vertrag ist mit jedem Anbieter einzeln abzuschließen.
- Beide Unternehmen müssen vorab prüfen, ob das geforderte Datenschutzniveau sichergestellt werden kann – und falls nicht, muss der Anbieter dem Auftraggeber dies mitteilen, woraufhin dieser den Vertrag aussetzen oder beenden muss!

Der Verantwortliche und der Anbieter müssen also eine „Einzelfallanalyse“ durchführen (Absatz 134 des Urteils), um zu prüfen, ob der Anbieter irgendwelchen nationalen Gesetze unterliegt, die gegen die DSGVO oder die Charta der Grundrechte der Europäischen Union verstoßen.

Anders formuliert: Auch die SCC dürften für europäische Unternehmen **keine ausreichende Grundlage** bieten, um personenbezogene Daten an einen amerikanischen Anbieter zu transferieren. Denn europäische Unternehmen müssen prüfen, ob diese in der Praxis von dem Anbieter überhaupt eingehalten werden können. Diese Prüfung wird wohl in der Praxis kaum durchführbar sein und die laufende Einhaltung der SCC zu kontrollieren wäre de facto unmöglich.

Der EuGH hat dabei betont, dass die Datenschutzbehörden die Pflicht haben, einzugreifen, um Datenübermittlungen auszusetzen oder zu verbieten (Randnummer 134 des Urteils), sollte ein gültiges Rechtsinstrument für eine Übermittlung fehlen und der Verantwortliche nicht tätig werden.

Ist nicht der Anbieter für die Einhaltung der SCC verantwortlich?

Ja und nein. Einerseits hatte der amerikanische Anbieter die Pflicht, seine Kunden über Überwachungsgesetze wie FISA zu informieren. Wenn er das nicht getan hat, stehen einige Juristen auf dem Standpunkt, dass der Anbieter für alle Kosten haftet, die sich aus der Aufhebung der SCC ergeben. Doch hier stellt sich die die Frage: Wie realistisch wird das in der Praxis durchsetzbar sein?

Und eines ist in der DSGVO ganz klar geregelt: Das Unternehmen (der „Verantwortliche") ist für die Einhaltung der DSGVO in letzter Konsequenz verantwortlich – auch für die Auswahl seines Anbieters. Dieser Verantwortung kann sich kein Unternehmen entledigen und wird daher auch für Verstöße gerade stehen müssen.

Betrifft das EuGH Urteil nur den Datentransfer in die USA?

Ja und nein. Das EuGH Urteil bezog sich auf das Privacy Shield Abkommen und dieses regelte ausschließlich den Datentransfer zwischen der EU und den USA.

Doch die grundlegenden Überlegungen dazu gelten für alle Drittländer außerhalb der EU (wie zum Beispiel Russland oder China, deren Datenschutz-Niveau ebenfalls von jenem in der EU abweicht).

Die Konsequenz des Urteils ist also: Unternehmen werden das tatsächliche Schutzniveau, das in Nicht-EU-Ländern herrscht, viel genauer als bisher überprüfen müssen. Denn jedes EU-Unternehmen muss prüfen, ob es in dem Drittland Gesetze gibt, die die europäischen Datenschutzbestimmungen außer Kraft setzen können. Falls ja, ist eine Übermittlung nicht ohne weiteres möglich.

Ist mein Newsletter davon betroffen?

Wenn Sie einen amerikanischen Dienstleister einsetzen, dann **eindeutig ja**. Denn bei E-Mail Marketing werden zwingend personenbezogene Daten (wie die E-Mail Adresse) übertragen.

Hier stellt sich einerseits die Frage, ob für einen Newsletter "zwingend notwendig" ein amerikanischer Anbieter eingesetzt werden muss; angesichts der Vielfalt an europäischen Alternativen ist das wohl zu verneinen.

Andererseits könnte der Anbieter über SCC (siehe oben) datenschutz-rechtliche Garantien abgeben. Wie oben ausgeführt ist allerdings mehr als fraglich, ob das eine ausreichende Grundlage für die Datenübermittlung in ein nicht-sicheres Drittland wie den USA darstellen kann.

Aber Mailchimp hat doch geschrieben...

In einem Statement an seine Kunden nahm Mailchimp zum Ende von Privacy Shield wie folgt Stellung:

> *"First, we want to reassure our customers that they can continue using Mailchimp lawfully and don't need to take any action. We have long provided our customers with two layers of protection for data transfers from the EU to the US in our Data Processing Addendum: compliance with the EU-US Privacy Shield Framework and Standard Contractual Clauses (SCCs).*
>
> *While the ruling from the CJEU invalidated the Privacy Shield Framework, it doesn't affect the SCCs, which remain a valid data export mechanism. Our agreements are structured in a way that the SCCs automatically take effect, so nothing will change for our customers."*

Diese Behauptung ("SCC remain a valid data export mechanism") ist laut aktueller Meinung der meisten Juristen **schlicht falsch.** Denn wie oben erklärt wurden die SCC zwar an sich vom EuGH als grundsätzlich zulässig bestätigt, jedoch verhindern die gleichen Gesetze, die das Privacy Shield zu Fall brachten, auch die Einhaltung der SCC.

Anders formuliert: Mailchimp gibt darin Versprechen ab, die das Unternehmen faktisch gar nicht einhalten kann, weil es nun einmal den amerikanischen Gesetzen unterliegt. Da die Kunden hier jedoch das Auswahlverschulden trifft und sie außerdem verpflichtet sind, zu überprüfen, ob die Datenschutzbestimmungen im Land des Anbieters (also den USA) eingehalten werden können, ist das aktuelle Risiko für den weiteren Einsatz von Mailchimp sehr hoch. Da nutzen auch die Versprechen des Anbieters wenig.

Und wenn die Server in Europa stehen?

Das macht keinen Unterschied. Denn amerikanische Behörden haben ja dennoch Zugriff auf die Daten über die verschiedenen Überwachungsgesetze der USA. Wo die Server physisch stehen, spielt dabei weder technisch noch faktisch eine Rolle.

Sind Partner-Agenturen von Mailchimp & Co. betroffen?

Agenturen und Berater, die bislang Mailchimp oder andere amerikanische Anbieter empfohlen oder eingesetzt haben, müssen ab sofort doppelt vorsichtig sein. Denn im worst case trifft sie die „Beraterhaftung".

Das bedeutet, dass die Agentur schadenersatzpflichtig wird, wenn sie einem Kunden ein System empfiehlt, von dem sie hätte wissen müssen, dass der Kunde es nicht legal einsetzen kann. Angesichts der empfindlichen Strafen, die in DSGVO vorgesehen sind, ist das finanzielle Risiko dementsprechend hoch.

Muss ich gleich mit hohen Strafen rechnen?

Vermutlich nicht. Das soll **kein Freibrief** sein, doch auch nach dem Urteil des EuGH zum Safe Harbor Abkommen agierten die Datenschutzbehörden eher zurückhaltend.

Auch nach dem Ende des Privacy Shield ist nicht zu erwarten, dass die Datenschutz-Behörden gleich mit Überprüfungen beginnen und noch weniger, dass bei Verstößen hohe Strafen verhängt werden.

Allerdings scharren wohl schon die ersten Abmahnanwälte in den Startlöchern. Und auch Betroffene (also zum Beispiel Newsletter-Empfänger) könnten eine Anzeige bei einer Datenschutz-Behörde überlegen, wenn ihnen klar wird, dass ihre personenbezogenen Daten ohne Zustimmung an einen amerikanischen Dienstleister geschickt wurden.

Wie hoch ist das Risiko und welche Konsequenzen drohen?

Europäische Unternehmen, die weiterhin unrechtmäßig Daten an US-Empfänger übermitteln, sind gut beraten, alle solchen Übermittlungen möglichst zeitnah zu überprüfen und ggfs. zu beenden (bzw. sich nach einer rechtlich einwandfreien Alternative umzusehen).

Denn die DSGVO sieht Geldstrafen von bis zu 20 Millionen Euro oder 4% des weltweiten Umsatzes vor.

Der EuGH hat außerdem ein Anrecht auf Ersatz für immateriellen Schaden in "abschreckender Höhe" definiert, sollten beim Umgang mit Daten von Nutzern Standardvertragsklauseln verletzt werden. Und er hat klargestellt, dass die nationalen Datenschutzbehörden hier eine Prüfung vornehmen müssen.

In Summe hat der EuGH also unmissverständlich klar gemacht: Die Nicht-Einhaltung der datenschutzrechtlichen Vorschriften, auch bei der Datenübermittlung in das EU-Ausland, ist kein Kavaliersdelikt.

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
© E-Mail Marketing Academy – alle Rechte vorbehalten.