von Rechtsanwalt **Phil Salewski**

Vorsicht bei Datentransfers an US-Dienste: BayLDA erklärt Nutzung von Mailchimp für grundsätzlich datenschutzwidrig

Ein Großteil der Online-Händler nutzt für Newsletter-Kampagnen die Dienste externer Serviceanbieter, welche die Organisation, Gestaltung und Versendung von Werbemails übernehmen. Fällt die Auswahl hier auf US-amerikanische Dienstleister, kann dies für europäische Online-Händler allerdings zum datenschutzrechtlichen Fallstrick werden. Nach Wegfall des EU-US-Privacy-Shield sind Datenübermittlungen an Newsletterversand-Dienstleister in den USA nicht mehr ohne Weiteres möglich. Dies belegt eindrucksvoll eine aktuelle Entscheidung des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) vom 15.03.2021, das einem Online-Händler aus Datenschutzgründen die Nutzung der Dienste von Mailchimp untersagte. Mehr zu den Details der Entscheidung und den Konsequenzen für den Online-Handel lesen Sie im folgenden Beitrag.

I. Was war passiert?

Am 16.07.2020 hatte der EuGH das sog. EU-US-Privacy Shield für ungültig erklärt. Dieses Datenschutzschild hatte bis dahin als Angemessenheitsbeschluss für die datenschutzrechtliche Konformität der Übermittlung personenbezogener Daten aus Europa in die USA gedient.

Hintergrund der Entscheidung war, dass selbst unter Beachtung aller Datensicherheitsbestimmungen des Datenschutzschildes ein Zugriff auf personenbezogene Datenbestände durch US-Behörden nicht ausgeschlossen werden konnte. Aufgrund nationalrechtlicher Ermächtigungen waren Datenauskunftsverlangen und deren Durchsetzung durch US-Nachrichtendienste möglich - ein großes Risiko für den Schutz von Daten aus Europa, wo entsprechende behördliche Ermächtigungsgrundlagen in dem Umfang nicht existieren.

Folge des Wegfalls des Privacy Shield war nun unter anderem, dass der Einsatz sämtlicher US-Dienste, die sich zuvor auf das Datenschutzschild gestützt hatten, in Europa grundsätzlich rechtswidrig zu sein drohte. Es fehlten nämlich geeignete Datensicherheitsgarantien für transatlantische Datentransfers.

Diverse Diensteanbieter aus den USA versuchten in den Folgemonaten, die entstandene Datenschutzlücke durch die Implementierung sogenannter Standardvertragsklauseln zu schließen - ein

grundsätzlich anstelle eines Angemessenheitsbeschlusses ebenfalls ausdrücklich (Art. 46 Abs. 2 lit. c DSGVO) anerkanntes Instrument für die notwendige Datensicherheit bei Datentransfers ins außereuropäische Ausland.

Speziell für die USA vermögen diese Klauseln das Kernproblem aber nicht zu beseitigen: Die Datenschutzklauseln verpflichten US-Diensteanbieter zur Einhaltung europäischer Datenschutzbestimmungen nur im Verhältnis zum Diensteempfänger, gelten also nur zwischen den Vertragsparteien. US-Behörden werden durch die Klauseln also nicht mitverpflichtet und können in ihren Zugriffsbefugnissen dadurch nicht beschränkt werden. Auch können die Standardklauseln Datenzugriffe der US-Behörden im Zweifel nicht verhindern. Sie können einem nach US-Recht legitimen Datenauskunftsverlangen einer US-Behörde nämlich nicht entgegengehalten werden.

Insofern besteht bei den EU-Datenschutzbehörden weitgehende Einigkeit darüber, dass die bloße Implementierung von Standardklauseln nicht ausreicht. Vielmehr wären weitergehende technische und organisatorische Maßnahmen erforderlich, mit denen die US-Anbieter Zugriffe auf EU-Datensätze verhindern. Diskutiert wird vor allem die hinreichende Verschlüsselung und/oder Pseudonymisierung von EU-Daten so, dass diese bei Zugriffen durch US-Behörden von jenen nicht ausgelesen werden könnten.

Standardvertragsklauseln nach EU-Vorbild allein sind in den USA also mehr Schein als Sein. Für sich genommen bieten sie die notwendige Datensicherheit gerade nicht.

Eben diese Schlussfolgerung wurde nun jüngst einem Münchner Online-Händler zum Verhängnis, der sich für den Versand von Newslettern der Dienste des US-Anbieters "Mailchimp" bediente.

Im Zuge der Beauftragung von Mailchimp wurden Mailadressen von EU-Bürgern an Server von Mailchimp in den USA übertragen, damit von dort aus der Newsletterversand organisiert werden konnte.

Mailchimp berief sich für derartige Datentransfers auf Standardvertragsklauseln, nachdem das Privacy Shield zu Fall gebracht worden war.

An der fehlenden Datensicherheit stieß sich daraufhin das Bayerische Landesamt für Datenschutzaufsicht.

II. Die Entscheidung des BayLDA in Bezug auf Mailchimp

Das BayLDA befand am 15.03.2021 Datenübermittlungen an Mailchimp für unzulässig, weil durch die Implementierung von Standardvertragsklauseln allein nicht ausgeschlossen werden könne, dass Mailchimp Datenzugriffen von US-Nachrichtendiensten unterfallen könne.

Eine Zusammenfassung der Entscheidung ist **hier** einsehbar.

Nach Ansicht des BayLDA hätte der betroffene Online-Händler im Zuge der Beauftragung von Mailchimp prüfen müssen, ob neben den Standardklauseln noch weitere Maßnahmen für die Datensicherheit hätten getroffen werden müssen.

Laut der Behörde war also nicht die Inanspruchnahme der Mailchimp-Dienste an sich datenschutzwidrig, sondern das Fehlen einer vom Online-Händler vorzunehmenden Interessen- und Risikoabwägung mit dem Ergebnis einer Entscheidung über weitere datenschutzrechtliche Sicherheitsmaßnahmen.

Weil es hieran fehlte und sich der Händler allein auf die Standardvertragsklauseln verlassen hatte, wurde ihm die Nutzung von Mailchimp untersagt.

Ein Bußgeld wurde gegen ihn aber nicht verhängt.

III. Das Unmögliche: Risikobewertungen durch Online-Händler selbst

Im Internet ist derzeit in vielen Artikeln zu lesen, dass die Entscheidung des BayLDA nicht missverstanden werden dürfe. Nicht die Nutzung von Mailchimp an sich, sondern erst eine fehlende Risikobewertung und die daraus folgende mangelnde Vornahme weiterer Maßnahmen machten die Datentransfers datenschutzwidrig.

Übersehen wird hierbei aber gerne, dass Online-Händler eine Datensicherheitsbewertung von US-Diensten nie möglich sein wird:

Einerseits halten sich die US-Dienste grundsätzlich bedeckt, was ihre Datenverarbeitungsprozesse angeht. Online-Händler haben also per se keine Möglichkeit, Art und Umfang aller Verarbeitungen korrekt zu erfassen.

Selbst aber, wenn dies im Einzelfall möglich wäre, fehlt Händlern andererseits jedoch die notwendige rechtliche Expertise, um die Bewertung zu einem tragbaren datenschutzkonformen Ergebnis zu bringen.

Schließlich ist zu befürchten, dass sich die US-Dienste, die im Vergleich zum Händler am deutlich längeren Druckhebel sitzen, kaum bereiterklären würden, auf Anfrage einzelner Akteure aus der Händlerschaft weitere Datenschutzmaßnahmen speziell für diese Individuen einzurichten.

IV. Konsequenz: Abstand von US-Diensten anzuraten

Ist Händlern die Risikobewertung einerseits und die Durchsetzung weiterer Datenschutzmaßnahmen gegenüber US-Diensten andererseits nicht möglich, entspricht die vom BayLDA bekundete Unzulässigkeit des "ungeprüften Einsatzes" eines US-Dienstes dem "grundsätzlichen Einsatz" desselben.

Das bedeutet: für Online-Händler sind Datenübermittlungen an US-Dienste, die sich allein auf Standardvertragsklauseln berufen, grundsätzlich unzulässig!

Die Entscheidung des BayLDA zu Mailchimp sollte also als unbedingter Anlass verstanden werden, Abstand von US-Services zu nehmen, die Datenübermittlungen voraussetzen.

Hierhin geht auch eine **aktuelle Stellungnahme des Datenschutzbeauftragten des Landes Baden-Württemberg**.

Datentransfers auf Basis von Standardvertragsklauseln in die USA sieht dieser nur dann als ausnahmsweise zulässig an, wenn eindeutig belegt werden kann, dass die US-Dienstleistung nicht kurz- oder mittelfristig durch eine zumutbare Alternative ohne Transferproblematik ersetzt werden kann, wenn also nicht kurz-oder mittelfristig eine gleichgelagerte Leistung eines EU-Anbieters oder eines Anbieters aus einem Land beauftragt werden kann, für das ein Angemessenheitsbeschluss vorliegt.

V. Fazit

Im Angesicht der jüngsten Entscheidung des BayLDA am Beispiel von "Mailchimp" sei Online-Händlern zwingend empfohlen, Datentransfers an US-Dienste einzustellen.

Die Übermittlung von Daten an Diensteanbieter aus den USA nur auf Basis von Standardvertragsklauseln muss nämlich als grundsätzlich datenschutzwidrig eingestuft werden.

Etwas anderes kann im Einzelfall ausnahmsweise und nur dann gelten, wenn eindeutig nachgewiesen kann, dass sich der US-Service nicht zumutbar durch ein europäisches oder ein Pendant aus einem Land ersetzen lässt, für das ein DSGVO-Angemessenheitsbeschluss vorliegt.

Ist die Dienstleistung in zumutbarer Weise ersetzbar, sind Datentransfers an den US-Dienst grundsätzlich unzulässig.

Autor:
RA Phil Salewski
Rechtsanwalt