Newsletter-Programm nicht DSGVO-konform wegen Privacy-Shield-Out!

Darf man überhaupt noch US-Software oder US-Dienstleister nutzen?

Der aktuelle Newsletter von meineberater.at informierte darüber, dass die **bayrische Datenschutzbehörde** (BayLDA) entschieden hat, dass das Newsletter-Programm **Mailchimp** nicht gesetzeskonform genutzt werden kann, denn diese Software **verletzt die DSGVO.**

Im Beitrag sehen wir uns den **konkreten Anlassfall** näher an und erklären, was es mit dem Privacy-Shield auf sich hat. Weiters informieren wir darüber, was dieses **Urteil für die Praxis bedeutet** (darf man nun US-Firmen nutzen oder nicht?) und verweisen auf eine **Checkliste,** die Ihnen bei der Frage helfen könnte, **ob ein Datentransfer in die USA oder Drittländer** (aus der Sicht der EU) **erlaubt ist oder nicht.**

Hintergrund: Durch die **Entscheidung des Europäischen Gerichtshof (EuGH),** dass das Privacy-Shield-Abkommen zwischen den USA und der EU als ungültig erklärt wurde, muss man sich **jede Software, jeden Dienstleister**, etc. genau ansehen, ob **Daten in die USA übertragen** werden.

Zum konkreten Anlassfall:
Mailchimp ist eine – besonders bei kleinen und mittelgroßen Unternehmen – beliebte Software, um Newsletter zu versenden. Problematisch aus Sicht der DSGVO ist, dass es sich hierbei um einen amerikanischen Dienst handelt.
Ein **Newsletter-Empfänger einer bayrischen Firma,** die Mailchimp nutzte, hat sich darüber bei der zuständigen Datenschutzbehörde beschwert.

Die exakte **Argumentation in der Beschwerde**, dass es nach dem Ende des Privacy-Shield-Abkommens **keine ausreichende Grundlage** gebe, um ohne Zustimmung der Betroffenen personenbezogene Daten wie etwa die E-Mail Adresse an ein amerikanisches Unternehmen zu übergeben, ist auf der Seite der E-Mail Marketing Academy und zwar hier nachzulesen…

Die Behörde prüfte, ob die Nutzung von Mailchimp durch das bayrische Unternehmen zulässig war. **Ergebnis: Nein, die Verwendung war datenschutzrechtlich unzulässig, d.h. entspricht nicht der DSGVO!**

Begründung: Das bayrische Unternehmen habe nicht geprüft, ob für die Übermittlung an Mailchimp zusätzlich zu den Standarddatenschutzklauseln noch **„zusätzliche Maßnahmen"** im Sinne der EuGH-Entscheidung „Schrems II" (EuGH, Urt. v. 16.7.2020, C-311/18) **notwendig sind,** um die Übermittlung datenschutzkonform zu gestalten, zitierten meineberater.at bzw. die E-Mail Marketing-Academy aus dem Urteil.
Den genauen Ablauf des Datenschutzverfahrens können Sie hier… nachlesen.

Folgen des Urteils: Man darf sich bei Datentransfer in die USA oder einen Drittstaat **nicht nur auf die Standardvertragsklauseln,** kurz SCC (Abkürzung für Standard Contractual Clauses) **verlassen.**

Die **Ursache für das Problem liegt** in den **unterschiedlichen Datenschutzansprüchen zwischen USA und EU.** In den USA hat man eine niedrige Anforderung, was den Datenschutz betrifft, besonders dann, wenn es sich um Daten von Europäern handelt. Und amerikanische Firmen sind nach diversen US-Gesetzen verpflichtet, **Geheimdiensten Zugang zu Daten zu gewähren.** Die Schlagworte dazu lauten etwa **Cloud Act oder FISA 702**. Einfach mal googlen, man kommt aus dem Staunen kaum raus…

Diese „Abhör"-Praxis in den USA führte zum Ende des **Privacy Shield**-Abkommens und dessen Vorgänger, nämlich dem **Safe-Harbour-**Abkommen. Beide Abkommen hat der österreichische Datenschützer Max Schrems zu Fall gebracht, mit dem Argument, dass das Recht und die Praxis der USA im Hinblick auf Datenzugriffe keinen ausreichenden Schutz vor dem Zugriff der Behörden bieten würde. Und tatsächlich wurde 2015 das Safe-Harbour-Abkommen und 2020 das Privacy-Shield-Abkommen **vom EuGH als ungültig erklärt.**

Ist Datentransfer in die USA grundsätzlich verboten? Was bedeutet das für die tägliche Praxis?

Nein, ein Datenaustausch mit den USA ist **nicht grundsätzlich verboten.**
Aber Fakt ist, die **USA gelten als unsicherer Drittstaat** und daher darf man sich nicht nur auf die sogenannten Standardvertragsklauseln (SCC) verlassen (siehe oben), d.h. nur „dank SCC" darf man keine Daten in die USA übertragen. Sondern man muss **jede einzelne US-Firma danach prüfen,** wie sie es mit dem Datenschutz konkret hält. Und etwa **zusätzliche Sicherheiten oder Garantien einholen**, etwa die Zusage, dass zum Beispiel Geheimdienste nicht auf die Daten zugreifen können, etc. Meist findet man das unter dem Schlagwort **„Binding corporate rules" auf den Webseiten,** was so viel heißt, wie verpflichtende firmeninterne Datenschutzvorschriften.

Allerdings hat auch dieser „Ausweg" einen **Pferdefuß:**
Denn es gibt noch keine Vorgabe, wie solche „zusätzliche Maßnahmen" konkret auszusehen haben. Es herrscht seit dem Ende des Privacy-Shield eine ziemliche Leere und damit verbundene Unsicherheit.

Und sich auf **„binding corporate rules" zu verlassen,** kann auch **problematisch** sein. Denn wie wollen Sie überprüfen, ob sich der Anbieter daran überhaupt hält? Und sollte er es nicht tun, sind Sie erst recht **(mit-) schuld,** weil Sie ihn als Lieferant ausgewählt haben, falls er dann doch nicht DSGVO-konform gearbeitet hat. Sehr mühsam und gefährlich. Droht doch in letzter Konsequenz das Damokles-Schwert in Form von **Strafen von bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes.**

Wem das oben beschriebene **Vorgehen zu mühsam** ist und wer es sich einfacher machen will, der sollte prüfen, ob es nicht etwa **europäische Alternativen gibt.** Das ist etwa beim Thema Newsletter-Versand durchaus einfach zu lösen. Auch Cloud-Anbieter kann man leicht durch europäische Firmen ersetzen. Schwieriger wird es wohl mit einigen „Monopolisten", an die wir uns in unserem Geschäftsleben schon allzu sehr gewöhnt haben. Etwa Microsofts Office Paket oder die vielen Google-Produkte, die auf vielen Computer vorzufinden sind, um konkrete Beispiele zu nennen.

Achtung: Zu diesem Problemkreis gibt es betreffend **Google Analytics eine topaktuelle Entscheidung:**
In einem Verfahren vor der österreichischen Datenschutzbehörde, das ebenfalls der Datenschutzverein von Max Schrems namens **noyb** (Abkürzung für none of your business, frei auf Deutsch übersetzt: Unsere Daten gehen euch nichts an…) angestrengt hat, musste Google zugeben, dass **bei der Nutzung von Google Analytics ALLE DATEN IMMER in den USA gespeichert werden**. Bisher hatten die Datenkraken immer argumentiert, dass sie einen Sitz in Irland hätten und nur diese Tochter die Daten verarbeiten würde, also alles innerhalb Europa bliebe. Diese Argumentation und damit die DSGVO-Konformität ist nicht mehr haltbar. ALSO HÄNDE WEG von Google Analytics.

Weitere entsprechende Entscheidungen werden wohl kommen. Aber es wäre zu hoffen, dass es bald eine **Nachfolge-Regelung zwischen EU und USA gibt,** unter welchen (einfacheren?) Voraussetzungen man wieder miteinander Daten austauschen darf.
Zum **Schluss noch ein Tipp:** Vielleicht ist der **Praxisleitfaden** von Meineberater.at für die tägliche Umsetzung obiger Fragen nützlich. Diesen finden Sie hier…

Gerne stehe ich für Anfragen auch in diesem Bereiche **für Zurich-Partner zum Spezialpreis** zur Verfügung.

Quellen und Mitarbeit: Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche (www.b2b-projekte.at), Newsletter von meineberater.at, Webseite des Bayrischen Landesamts für Datenschutzaufsicht und der E-Mail Marketing Academy, Computerwelt

RA Mag. Stephan Novotny
Weihburggasse 4/2/26
1010 Wien

kanzlei@ra-novotny.at

www.ra-novotny.at

PS: Gerne stehe ich den Zurich-BAV-Newsletter-Lesern bei Rückfragen, Beratungen, Vertretungen unter **Hinweis „Zurich"** zum Sonderpreis zur Verfügung!