Rechtskonforme MailChimp-Nutzung nach Wegfall des EU-US-Privacy-Shields

Betrachtungen zur aktuellen Diskussion um die Verwendung von MailChimp als Newsletter-Tool

(Zusammengestellt von: Rudolf Urban und Walter Wratschko, 08.04.2021)

Ausgangslage

Die Datenschutzbehörde in Bayern behandelte vor Kurzem die Beschwerde eines Betroffenen, der die Weitergabe von Daten an die Newsletter-Plattform MailChimp kritisierte, und stellte im konkreten Fall am 15.03.2021 fest, dass die Übermittlungen personenbezogener Daten in die USA unzulässig waren. Darüber haben zahlreiche Medien, unter anderem “Der Standard”, berichtet.

Da uns bekannt ist, dass zahlreiche Unternehmen in Kärnten und Österreich den Newsletter-Versand über das Newsletter-Tool MailChimp realisiert haben, zeigen wir hier kurz auf, wie Unternehmen ihren Newsletter-Versand so risikofrei und gesetzeskonform wie möglich gestalten können.

Diese Erstinformation soll einen Überblick zum Thema geben. Die Interpretationen des Beschlusses durch die Medien sind jedenfalls in einigen Punkten zu hinterfragen.

Grundsätzlich hat die Datenschutzbehörde in Bayern entschieden, dass der verantwortliche Betreiber, der MailChimp genützt hat, seine Verpflichtung zur Prüfung der Rechtslage nicht ordnungsgemäß erfüllt hat, weil er neben der Berufung auf die Standarddatenschutzklauseln keine zusätzlichen Maßnahmen geprüft hat, um die Übermittlung datenschutzkonform zu gestalten. Eine solche Prüfung, wie unten beispielhaft angeführt, ist nach dem einschlägigen EuGH Urteil Schrems II jedoch unumgänglich.

Mögliche Maßnahmen

Um die Datenverarbeitung im gegenständlichen Fall ausführlicher zu prüfen, wären einige Fragen zu behandeln, z.B.:

Erstens, ob es andere, gleich gut funktionierende Tools gibt, die mit denselben personellen, technischen oder finanziellen Ressourcen für eine Newsletter-Versendung genützt werden könnten. Diese Einschätzung hat das Unternehmen zu machen. Wenn die Alternativen schwierig zu bedienen, teurer oder nicht so funktionell wären, wären diese Fakten und Argumente zu bewerten und zu dokumentieren.

Die zweite Prüffrage ist, ob die Newsletter-Versendung mittels MailChimp wegen der Verarbeitung in den USA eine risikobehaftete Verarbeitung ist oder sein kann. Zu fragen wäre sinngemäß, ob deswegen, weil die E-Mail-Adressen der Newsletter-Empfänger in den USA durch Behörden abgefragt würden, nachteilige Effekte auf diese Newsletter-Empfänger entstehen könnten. Problematisch könnten z.B. Inhalte sein, die dazu führen könnten, dass die USA daran Interesse haben könnten, z.B. politische Positionen, kriminelle Machenschaften usw. Dies ist in den meisten Fällen aufgrund der üblichen Inhalte eines Unternehmens-Newsletters nicht zu erwarten.

Die alleinige Information darüber, dass ein Newsletter bezogen wird, lässt wohl keine negativen Rückschlüsse zu und kann wohl kaum zu irgendwelchen Schäden (z.B. wirtschaftlichen oder persönlichen Nachteilen wie Flugverboten, Einreiseverboten, Imageverlusten usw.) führen.

Die dritte Frage, die behandelt werden muss, ist, welche Datenschutzmaßnahmen von MailChimp getroffen werden und welche Rechtsgrundlage(n) der Verarbeitung zugrunde liegen. Im konkreten Fall ist der automatisch abgeschlossene Verarbeitungsvertrag zu erheben und die damit vereinbarten Standardvertragsklauseln.

MailChimp erläutert dies in seinem Dokument „Data Processing Addendum“. Bei MailChimp gibt es besondere Sicherheitsmaßnahmen, wie eine Verschlüsselung nach dem Stand der Technik und es gibt die Zusicherung, dass die Anfragen der Behörden auf ihre Zulässigkeit geprüft werden. MailChimp veröffentlicht sogenannte Transparenzberichte, aus denen hervorgeht, wie häufig es zu Anfragen durch Behörden gekommen ist.

Tatsächlich wurden nur eine geringe Anzahl von Behörden- und Gerichtsanfragen beantwortet, wobei vielfach keine Informationen erteilt wurden. Für 2018 gab es gemäß Transparenzbericht insgesamt 20 Anfragen, davon wurden in 7 Fällen keine Informationen übergeben. Eine Informationsweitergabe erfolgte wie folgt: in 10 Fällen mit Daten zum Kontoinhaber und in 3 Fällen sowohl mit Daten zum Kontoinhaber als auch mit Inhaltsdaten der versendeten Nachrichten, davon in 1 Fall mit Zustimmung des Users. Im Jahre 2019 gab es insgesamt 18 Anfragen, davon wurden in 9 Fällen keine Informationen übergeben. Eine Mitteilung erfolgte wie folgt: in 9 Fällen mit Daten zum Kontoinhaber und in keinem Fall sowohl mit Daten zum Kontoinhaber als auch mit Inhaltsdaten der versendeten Nachricht. Es gab auch 2 Anfragen aus dem USA-Ausland, und zwar eine Anfrage aus Indien und eine Anfrage aus Malta – bei beiden wurden keine Informationen offengelegt. Beim enormen Umfang der Newsletter-Versendungen über MailChimp erscheint dies minimal.

Datenschutzrechtliche Beurteilung

Eine Beurteilung der Tauglichkeit von MailChimp für einen datenschutzkonformen Betrieb kann aufgrund einer solchen Analyse erfolgen. Diese muss dokumentiert sein, besonders für den Fall, dass man eine Beschwerde eines Betroffenen bei der Datenschutzbehörde zu behandeln hätte.

Ein Unternehmen, das sich diese Informationen und Argumente ansieht, kann zum Schluss kommen, dass mit den getroffenen Maßnahmen, weil diese ausreichend sind, ein angemessenes Schutzniveau gewährleistet ist.

Zu den zusätzlichen Maßnahmen werden vom Europäischen Datenschutzausschuss Empfehlungen, sogenannte „Supplementary Measures“, für die Übermittlung von personenbezogenen Daten in Drittländer ausgearbeitet, die derzeit aber noch Gegenstand der öffentlichen Konsultation sind. Nach Vorliegen dieser Empfehlungen muss die Sachlage neuerlich evaluiert werden.

Das Medienecho der Entscheidung der Datenschutzbehörde in Bayern ist zwar groß, es könnte aber auch beabsichtigt sein, in der Öffentlichkeit Druck aufzubauen, damit mehr europäische Dienstleister zum Zug kommen. Die Diskussion darüber hat jedenfalls Fahrt aufgenommen.

Grundsätzlich gilt, dass die Argumentation bezüglich der Pflicht zur Prüfung zusätzlicher Maßnahmen zu den Standardvertragsklauseln für **alle** Tools, welche von US-amerikanischen Herstellern betrieben werden, gilt. Also insbesonders auch Anwendungen wie Microsoft 365, Azure-Cloud, AWS Cloud, Google Workspace usw.

Der Betreiber muss sich jedenfalls ein Bild über die geltenden rechtlichen Rahmenbedingungen machen. Die Bedingungen, die für MailChimp gegeben sind, sind aber auch generell auf andere US-Tools anwendbar. Eine prinzipielle DSGVO-Nichtkonformität für alle US-Dienste, wie es von manchen DatenschutzexpertInnen formuliert wird, ist unserer Meinung nach nicht gegeben. Sehr wohl ist es aus unternehmerischen Gründen, wie zum Beispiel der Sicherung der Nachhaltigkeit der Investitionen in die betriebseigene IT-Infrastruktur, angesagt, sich nach europäischen Alternativen umzusehen.

Informationspflichten

Wichtige inhaltliche Themen dazu sind die Ausgestaltung der Information zum Datentransfer in der Datenschutzerklärung und die Ausgestaltung der Newsletter-Anmeldung mit Double-Opt-In sowie die Gestaltung der Einwilligungserklärung inklusive Aufklärung über die Verarbeitung in einem unsicheren Drittland.

Aufgrund der gegebenen datenschutzrechtlichen Informationspflichten haben die verantwortlichen Betreiber von US-Newsletter-Tools also seit dem bayrischen “Mailchimp-Beschluss” zwei dringende Handlungsnotwendigkeiten, und zwar:

Erstens ist bei sich neu eintragenden Newsletter-InteressentInnen ein wahrnehmbarer Hinweis, welches nichteuropäische Tool genutzt wird und welches Rest-Sicherheitsrisiko für die dort hinterlassenen personenbezogenen Daten besteht, anzuführen. Wenn der/die Interessent/in sich dann einträgt, hat er die explizite willentliche Zustimmung zur Nutzung dieses Tools gegeben.

Zweitens sollte den bestehenden Newsletter-Empfängern ehestmöglich ein separater Newsletter, welcher nur die Informationen bezüglich des Tools und die entsprechenden Sicherheitsthemen beinhaltet, zugesendet werden, wobei auch ein Hinweis auf die Möglichkeit des Opt-Out in diesem Newsletter zu geben ist.

Diese Handlungsempfehlungen sind wohl auch bei allen anderen US-Tools sinngemäß notwendig, um die eindeutige Rechtsgrundlage wieder herzustellen.

Aus Sicht des E-Mail-Marketings ist darüber hinaus noch an mögliche ablehnende Reaktionen der betroffenen Newsletter-Empfänger zu denken. Wer also weniger Absprung-Möglichkeiten für seine Leads in seiner Webpräsenz haben will, sollte sich für europäische Tools entscheiden, denn bei diesen kann die explizite Nennung der verwendeten Lösung und die Zustimmung zum Tool ja entfallen.

Fazit

Es ist die Entscheidung des jeweiligen Unternehmens, ob es MailChimp nützen und sich mit der arbeitsaufwendigeren Rechtslage auseinandersetzen möchte oder ob es sich mit dem Wechsel zu einem EU-Anbieter diese Arbeit erspart. Beides lässt sich so gestalten, dass es datenschutzrechtlich akzeptabel ist, wobei trotz aller Argumente beim Einsatz von US-Dienstleistern ein Restrisiko verbleibt, dass das Unternehmen zu tragen bereit sein muss. Übrigens: die bayerische Datenschutzbehörde verhängte wegen des behandelten Verstoßes keine Strafe, vorwiegend, weil nur wenige E-Mail-Daten betroffen waren, weil die Sensibilität von E-Mail—Adressen noch verhältnismäßig überschaubar ist und weil das Unternehmen den weiteren Versand mit MailChimp beendet hat. Insbesondere die Einschätzung der Behörde, dass E-Mail-Adressen eine noch verhältnismäßig überschaubare Sensibilität besitzen, erscheint für die weiteren zukünftigen datenschutzrechtlichen Betrachtungen von Bedeutung.

Die Datenschutzerklärungen vieler Unternehmen erläutern den Umgang mit weiteren US-Tools und deren Datenübermittlungen in die USA, beispielsweise Google, Facebook, Youtube, Instagram usw. Auch zu diesen Datenverarbeitungen sind entsprechend gestaltete Dokumentationen und Informationen gemäß Art 13 DSGVO in der hier beschriebenen Form erforderlich.

Für Fragen stehen wir jederzeit zur Verfügung.

Rudolf Urban und Walter Wratschko

Geprüfte Datenschutzexperten